(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 June 2006 (01.06.2006)

PCT

(10) International Publication Number
WO 2006/058119 A1

(51) International Patent Classification:
E05B 41/00 (2006.01) *G11B 33/04* (2006.01)
E05B 73/00 (2006.01) *E05B 47/00* (2006.01)
G01V 8/14 (2006.01)

(21) International Application Number:
PCT/US2005/042536

(22) International Filing Date:
23 November 2005 (23.11.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/630,452	23 November 2004 (23.11.2004)	US
60/644,197	13 January 2005 (13.01.2005)	US
60/730,585	26 October 2005 (26.10.2005)	US

(71) Applicant *(for all designated States except US)*: **AUTRONIC PLASTICS, INC.** [US/US]; 29 New York Avenue, Westbury, NY 11590 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LAX, Michael, R.** [US/US]; 1303 Ridge Road, Syosset, NY 11791 (US). **KEUNING, Timothy** [US/US]; 116 Makamah Road, Northport, NY 11768 (US). **VAN KOOT, Frederick** [US/US]; 8 Noyes Lane, Halesite, NY 11743 (US).

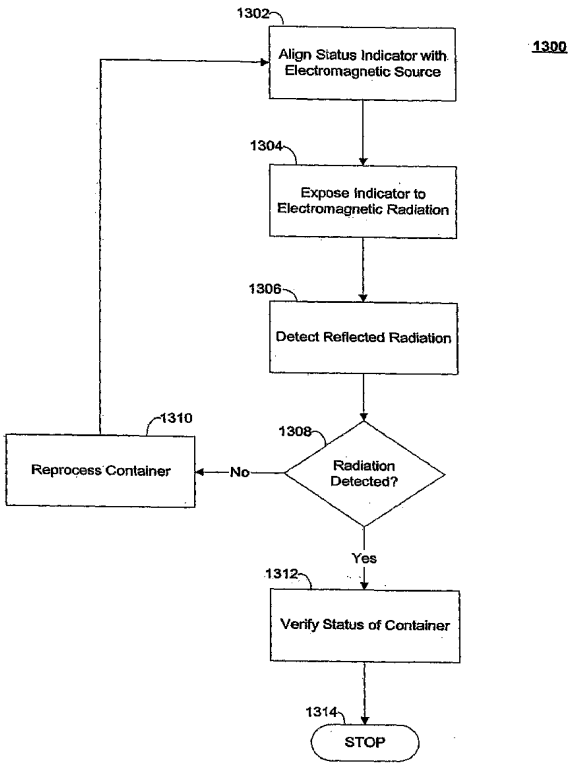
(74) Agents: **INGERMAN, Jeffrey, H.** et al.; c/o Fish & Neave IP Group of Ropes & Gray, 1251 Avenue of The Americas, New York, NY 10020 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR PROCESSING ITEMS



(57) Abstract: Apparatus and methods for processing assets in a lockable container are disclosed. A decoupler receives information from the container or the asset in the container. The container may be associated with a security status, and the item may be associated with a processing status. The decoupler may move the container along a processing path in a sequence based on the security status of the container and/or the processing status of the asset. The decoupler may also lock or unlock the container while moving the container along the processing path. At least a portion of the processing path may be exposed to a magnetic field, which may lock or unlock the container and/o activate or deactivate a security tag associated with the container or the item. The decoupler may also write or read information to or from an RFID tag associated with the container and/or the asset. This information may be used in conjunction with benefit denial, audit, loss prevention, transaction management, and other similar systems.

WO 2006/058119 A1

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

APPARATUS AND METHOD FOR PROCESSING ITEMS

Cross-References to Related Applications

[0001] This application claims the benefit of U.S. Provisional Applications Nos. 60/630,452, filed November 23, 2004, 60/644,197, filed January 13, 2005, and 60/730,585, filed October 26, 2005. The aforementioned earlier filed applications are all hereby incorporated by reference herein in their entireties.

Background of the Invention

[0001] The present invention relates generally to the field of retail and consumer merchandising, and more particularly to apparatus and methods for automated processing of retail and consumer merchandise in lockable containers.

[0002] The process of retail checkout is often a source of frustration for the consumer. Typically, retail checkout involves long wait times and interaction with inefficient or inexperienced retail

clerks. In some instances, consumers must wait for several minutes to process a single item at checkout.

[0003] In addition, conventional checkout techniques are typically not integrated with inventory control or product activation. For example, security and audit tags, such as electronic article surveillance ("EAS") tags, typically are manually removed or deactivated at checkout by the retail clerk using a separate process. This results in audit and security tags being unintentionally left behind on purchased merchandise. A security tag that is left on merchandise not only frustrates the consumer, who has to return to a retail clerk to have the tag removed or deactivated, but also decreases productivity and checkout efficiency.

[0004] There is a general trend toward self-checkout in retail stores, libraries, and rental locations, allowing consumers to buy or rent a product with nominal wait times. Self-checkout allows consumers to expedite their checkout process and partially or completely remove the interaction with the retail clerk. Some of the these self-checkout systems integrate payment with the self-checkout process, as with conventional grocery self-checkout terminals.

[0005] Such systems may also process merchandise protected with a benefit denial device. These systems provide a consumer with a physical asset at a point of sale (which, as used herein, will also include a "point of rental" or any other distribution or return point). The consumer then uses security information to obtain a benefit from the asset. A benefit denial device may deny a benefit to an unauthorized asset user and provide the benefit or permit access to the benefit to an authorized asset user.

[0006] The security information may be provided to the consumer at the point of sale. The security information may be stored with the asset in a form that is unusable by or inaccessible to the consumer until the consumer pays for the asset. The consumer is thus denied a benefit of the asset until the consumer has purchased or rented the asset. An entity that holds a right, such as an ownership right, in the asset is called a rights holder or content provider. The rights holder or content provider conveys a right to the consumer and is thus provided with protection against piracy and unauthorized reproduction of the benefit. This is because, in some instances, a pirate would be required to obtain the security information before acquiring the benefit. Furthermore, if a pirate were to sell unauthorized copies of the asset and provide buyers with security information, the rights holder or content provider could deny the benefit to buyers who use duplicated security information or security information corresponding to a stolen asset. This is often the case with software products that require product activation over the Internet or telephone with a unique product key.

[0007] An asset may include, for example, consumer electronics, cosmetics, an audio cassette, a CD, a CD-ROM, a video cassette, a DVD or a mini DVD, or any other asset capable of being stored in a storage case or container. The storage case may be displayed in an environment in which potential customers, renters, or users pick up and examine the storage case to determine whether they are interested in buying, renting, or otherwise acquiring the asset.

[0008] Known benefit denial systems for assets require security information to be stored on a card. The card must be "swiped" at the point of sale. Swiping a card is time-consuming and decreases the efficiency of point-of-sale processes such as check-out. The card is also exposed to viewing and tampering. Tampering may defeat the effectiveness of a benefit denial system.

[0009] In addition, the return of an asset in a container, particularly a rental asset in a container, poses several problems for the retailer. The retailer must manually process and restock the returned asset. Typically, this involves reactivating an EAS or other similar security device, locking the asset container, resetting the benefit denial device, and restocking the container on the sales or rental floor. This process can be time-consuming and tedious for the retailer.

[0010] In view of the foregoing, it would be desirable to provide improved apparatus and methods for processing and returning items at a point of sale quickly and efficiently.

[0011] It would be further desirable to provide apparatus and methods for preventing tampering with a device that retains security information.

[0012] It would be further desirable to provide apparatus and methods for verifying the security status of a container before the container leaves the retail or rental location.

[0013] It would be still further desirable to provide apparatus and methods for reducing risk of economic loss to an entity selling or renting an asset.

Summary of the Invention

[0014] In accordance with principles of the invention, systems and methods for processing an asset in an asset container are provided. The asset container may be received by a decoupler assembly, which may move the asset through a processing path based on information received from at least one of the asset container and the asset within the container.

[0015] In some embodiments, the decoupler may lock and/or unlock the asset container while moving the asset through the processing path. The decoupler may separately process the asset for sale, rental, loan, or return. To lock and/or unlock the container, the decoupler may pass the asset container through one or more magnetic fields. After locking or unlocking the container, the security status of the container may be verified by detecting reflected electromagnetic radiation from a portion of the container. In some embodiments, the decoupler may optically scan the container to verify that the container was successfully processed.

[0016] In some embodiments of the invention, an apparatus for use with a benefit denial system is provided. The apparatus may include a containing element configured to receive an asset. The asset may include a benefit for a user of the asset. The apparatus may include an electrical or RFID circuit that includes an antenna and is operatively associated with the containing element and configured to communicate information corresponding to the asset to a receiver outside the containing element. The information may be configured to be used by the benefit denial system to provide the benefit to the user.

[0017] In some embodiments of the invention, a container for use with a system for executing a conveyance of an interest in an asset from a first party to a second party is provided. The container may include a containing element configured to receive the asset and an electrical or RFID circuit operatively associated with the containing element and configured to communicate information corresponding to the asset to a receiver outside the containing element. The information may be configured to be used by the system to execute the conveyance.

[0018] In some embodiments of the invention, a container for an asset is provided. The container may include a containing element configured to receive the asset and an electrical or RFID circuit attached to the containing element and/or the assert and configured to communicate information corresponding to the asset to a receiver outside the containing element. The invention may include a circuit deactivator configured to interrupt electrical communication within the circuit.

[0019] In some embodiments of the invention, a locking member for use with 1) a benefit denial system; and 2) a lockable container, including an integral, internal locking member, is provided. The locking member may include an electrical circuit configured to communicate information associated with the asset to a receiver outside the container. The locking member or the container may include a security status indicator configured to close an optical circuit between the indicator and an optical sensor used to verify the security status of the container.

[0020] In some embodiments of the invention, a method for providing a benefit of an asset to an asset

user may be provided. The method may include receiving asset identification information transmitted by an antenna enclosed in a containing element and providing access information corresponding to the asset identification information to the user. The access information may be configured to provide the user with access to the benefit.

[0021] In some embodiments of the invention, a method for processing a container may be provided. The container is engaged with a container transport assembly. Status information is received from the container and/or the asset within the container. After receiving the information, the container may transported along a processing path in a sequence based on the received information. The processing path may alter the security information associated with the container.

[0022] In some embodiments of the invention an apparatus may be provided for processing an item in a lockable container. The apparatus may engage the lockable container with a container transport assembly and receive status information from the container and/or the asset within the container via a receiver. The apparatus may then transport the container along a processing path in a sequence based on the received status information. In some embodiments, the processing path may alter the status information associated with the container and/or the asset within the container. The processing path may expose at least a portion of the lockable container to a magnetic field. In some embodiments, this field may be used to lock or unlock the lockable container. In other

embodiments, the field may also activate or deactivate a security tag associated with the container.

[0023] In some embodiments of the invention a lockable container for securing an asset may be provided. The container includes a first cover and a second cover. The first and second covers are configured to move between an open position which allows access to the asset, and a closed position which prevents access to the asset. The container also includes a locking member that is configured to move between an unlocked position in which the first and second covers can move to the open position and a locked position which locks the first and second covers in the closed position. The locking member may include a security status indicator that is indicative of the security status of the container. The security status indicator may exhibit two positions. In one position the indicator is configured to close an optical circuit between an optical sensor and the indicator and in another position the indicator is configured to open the optical circuit with the optical sensor.

[0024] In some embodiments of the invention a method for verifying the security status of a lockable container containing a security status indicator may be provided. The security status indicator may be aligned with an electromagnetic radiation source. The indicator may then be exposed to the electromagnetic radiation source and reflected electromagnetic radiation may be detected. The security status of the container may then determined from the detected reflected electromagnetic radiation.

Brief Description of the Drawings

[0025] The above and other objects and advantages of the invention will be apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

[0026] FIG. 1A shows an illustrative lockable container in accordance with one embodiment of the invention;

[0027] FIGS. 1B and 1C are perspective views of an illustrative locking member for use with the lockable container of FIG. 1A in accordance with one embodiment of the invention;

[0028] FIG. 2A is an illustrative schematic diagram of apparatus, systems, and information in accordance with one embodiment of the invention;

[0029] FIG. 2B is another illustrative schematic diagram of apparatus, systems, and information in accordance with another embodiment of the invention;

[0030] FIG. 3 is a simplified top view of the transport chassis of the decoupler of FIG. 2 in accordance with one embodiment of the invention;

[0031] FIG. 4 is a simplified bottom view of the transport chassis of the decoupler of FIG. 2 in accordance with one embodiment of the invention;

[0032] FIG. 5 is a simplified top view of the main chassis of the decoupler of FIG. 2 in accordance with another embodiment of the invention;

[0033] FIG. 6 is a simplified diagram of the decoupler assembly in accordance with another embodiment of the invention;

[0034] FIG. 7 is a simplified bottom view of the flip cover of the decoupler assembly shown in FIG. 6 in accordance with another embodiment of the invention;

[0035] FIG. 8 is a diagram of another illustrative container for use with the decoupler assembly of FIG. 6 in accordance with another embodiment of the invention;

[0036] FIG. 9 is a diagram of yet another illustrative container for use with the decoupler assembly of FIG. 6 in accordance with another embodiment of the invention;

[0037] FIGS. 10A and 10B are diagrams of illustrative security status indicators of the containers of FIGS. 8 and 9 in accordance with one embodiment of the invention;

[0038] FIGS. 11A and 11B are diagrams of illustrative reflective security status indicators of the containers of FIGS. 8 and 9 in accordance with one embodiment of the invention;

[0039] FIG. 12 is a flow chart of an illustrative process for processing an item in accordance with one embodiment of the invention;

[0040] FIG. 13 is a flow chart of an illustrative process for verifying the security status of a container in accordance with one embodiment of the invention; and

[0041] FIGS. 14 and 15 show a user rendering a tag associated with a lockable container inoperable by tearing the tag in accordance with one embodiment of the invention.

Detailed Description of the Preferred Embodiments

[0042] In some embodiments, the invention may provide an apparatus for use with a benefit denial

system. The apparatus may include a containing element, such as a lockable container, that is configured to receive an asset. The asset may include a benefit for a user of the asset, such as electronic data encoded within or on the asset. For example, the asset may include encoded data, music, video, games, etc. In some embodiments, the assert may take the form of a CD, DVD, video or audio cassette, or any other asset capable of being contained within a containing element.

[0043] The containing element may include an electrical circuit for communicating information via an antenna to a receiver outside the containing element when the containing element is closed. The circuit may be disposed within or on the containing element, on the asset, or both. The circuit may communicate information to the receiver when the containing element is closed. The circuit may also communicate information to the receiver when the asset is enclosed inside the containing element or when the asset is locked inside the containing element. In some embodiments, the electrical circuit is also capable of receiving information from the receiver. In these embodiments, the receiver acts as both a receiver and a transmitter, and the electrical circuit may include receiver and transmitter circuitry.

[0044] In some embodiments, the electrical circuit communicates via RF signals. The circuit may include an RFID tag, RF transponder, RF transceiver, electronic product code (EPC) tag, reader, or any other component of an automated data collection (ADC) system that enables wireless capture and transmission of data using radio waves. The electrical circuit may include one or

more active or passive RFID tags. For example, if the circuit includes an active tag, the antenna associated with the tag may continuously emit data in the form of radio signals. Typically, the active tag may require a power source, such as a battery. If the circuit includes a passive tag, the tag may be interrogated by the receiver (or reader), which may also supply power to the electrical circuit.

[0045] The information read from or written to the electrical circuit may be configured to be used by the system to provide the benefit to the user. The information may be required by the system to provide the benefit to the user.

[0046] The apparatus may include a locking element configured to lock the containing element in a closed state. In some embodiments, the electrical circuit may be affixed to the locking element. In other embodiments, the electrical circuit may be affixed to the containing element, the asset, or both the containing element and the asset.

[0047] Examples of an asset containing element and apparatus for locking the containing element are shown and described in U.S. Patent Application Publication Nos. 2002/0023853, 2003/0000856, 2003/0111367, and 2004/0129587, all of which are hereby incorporated by reference herein in their entireties.

[0048] The examples include locking members that are operated by inserting the locking member into, and removing the locking member from, the containing element. The examples also include locking members that are internal to the containing element and are operated by moving the locking member from one position inside the containing member to another.

[0049] The circuit may include a data storage device. This device may be an integrated circuit chip and may be largely programmable. The digital storage device may be any suitable device and may include, for example without limitation, one or more of erasable programmable read-only memory, programmable read-only memory, read-only memory (ROM), electrically erasable read-only memory, random access memory (RAM), and hybrid types of memory. The circuit device itself may include an integrated circuit chip. The digital storage device may include asset identification information associated with the asset in the containing element, price information, security information, or any other related information.

[0050] In some embodiments of the invention, one circuit may be included in an EAS tag. The EAS tag may be configured to trigger an alarm if an article to which the tag is attached is moved into proximity with a detector that senses the presence of the tag.

[0051] In embodiments in which the electrical circuit is affixed to the locking element, the data storage device may be a reprogrammable, reburnable, or rewritable device. Reprogrammable or reburnable devices may be reprogrammed or reburned, respectively, to reconfigure the electrical circuit to communicate information associated with a different asset. For example, a first asset may be removed from the containing element and a second asset may be placed in the containing element. If so, the electrical circuit may be reconfigured to communicate information associated with the second asset.

[0052] The circuit may include an antenna, which may be any suitable antenna, including without limitation

any suitable dielectric resonator of any suitable geometry. The circuit may include or be part of a contactless smart card such as that sold under the name GemEasy 8000 by Gemplus Corp. of Horsham, Pennsylvania. The circuit may include or be part of a contactless smart object such as that sold under the name MA8000 by Gemplus of Horsham, Pennsylvania.

[0053] The asset and/or the containing element may have a type. For example without limitation, the asset may be a compact disc, a digital video disc, a digital versatile disc, a memory card, a memory cartridge, a memory chip, or any other suitable data storage or recording medium. In some embodiments, the asset may be a consumer product. The apparatus may be configured to enclose no more than three assets of a type. The apparatus may be configured to enclose no more than two assets of a type. The apparatus may be configured to enclose no more than one asset of a type.

[0054] The asset and/or containing element may also be associated with a processing status. In some embodiments, the processing status may indicate whether the asset is available for processing (e.g., able to be purchased, rented, loaned, or returned). The processing status may also include asset identification information, such as the asset title, description, price, or any other suitable information. If the asset is a rental asset, the processing status may also include information relating to the last or current renter, rental return dates, location where the asset was rented, location where the asset is to be returned, or any other suitable information.

[0055] The benefit associated with asset may include any suitable product or service. For example, the

benefit may include electronic or digital data, an executable computer program, an electronic game, audio, video, graphics, or any other benefit. In some embodiments, the benefit may include data that is inactive before the system receives a portion of the information. Inactive data may be unusable until it is activated. The system may be configured to activate the data.

[0056] The data may be configured to be accessed using an access device. The access device may be, for example without limitation, a personal computer, a work station, a mobile telephone, a personal data assistant, a game system (for example, without limitation, systems such as those sold under the trademarks GAMECUBE and GAMEBOY, by Nintendo of America, Inc. of Richmond, Washington; PLAYSTATION, by Sony Corporation of America, Inc. of New York City, New York and XBOX, by Microsoft Corporation of Redmond, Washington) and any other suitable access device. In some embodiments, the access device may require at least a portion of the information to provide the benefit to the user.

[0057] In some embodiments of the invention, the apparatus may be configured to provide a data key to the device. In some embodiments of the invention, the user may request the data key from the apparatus via telephonic communication. The telephonic communication may include voice communication. The telephonic communication may include telephone keypad tones. In response to the request, the apparatus may provide the data key to the user. The user may communicate the data key to the access device.

[0058] The data key may be configured to activate the data and may include activation data. In some

embodiments, the data key may be a file that is required before the user may obtain the benefit from the asset. The file may be an executable, non-executable, read-only, or read-write file. The file may also be encrypted. If the filed in encrypted, the file may include decryption information and/or one or more license numbers for one or more user licenses. Each license may entitle the user to obtain the benefit. In some embodiments, each license may entitle the user to obtain only a portion of the benefit. Multiple licenses may be aggregated to obtain a larger portion of the benefit. For example, one license may allow read-only access to the benefit, while another license may allow read-write access to the benefit. Multiple licenses may be combined to obtain the complete benefit. Alternatively or additionally, a license may require that the user obtain the benefit using a single access device. The access device may be identified to the system by the user, or the access device may identify itself to the benefit denial system.

[0059] In some embodiments, the apparatus may be configured to receive user information in the form of user input. The user information may include security data configured to be communicated by the user to the system. The security data may include an access code or a personal identification number (hereinafter, "PIN"). The information may include encoded letters, numbers, or any other suitable symbols. The system may also receive other user input, such as purchase or account information.

[0060] The information received or transmitted by the system may include transaction data configured to

be communicated by the receiver to the apparatus. The transaction data may be communicated to the system to confirm that the asset was conveyed to the user via an authentic transaction. As used herein, an authentic transaction may be a transaction that is authorized by an entity that owns or possesses or is conveying a copyright, patent right, trademark right, trade secret, or other right or intellectual property right in the asset. The transaction data may include data related to the sale or rental of the asset, including price and availability information.

[0061] The containing element may include optically opaque material. The optically opaque material may make it impossible for a viewer to perceive the presence or location of the circuit inside the containing element. In some embodiments, the containing element may be entirely opaque.

[0062] In some embodiments, the invention may provide a container for use with a system for executing a conveyance of an interest in an asset from a first party to a second party. The container may include a containing element configured to receive and enclose the asset. The container may also include an electrical circuit configured to communicate information corresponding to the asset to a receiver located outside the containing element when the containing element is closed. The circuit may disposed within the containing element, on the asset, or both. The information may be configured to be used by the system to execute the conveyance.

[0063] The circuit may be configured to communicate the information when the asset is enclosed within the containing element. The circuit may also be configured

to communicate the information when the asset is locked in the containing element. The information may include status information indicating the presence or absence of the asset in the containing element. For example, electrical circuits on both the container and the asset may both be configured to transmit information to the receiver. The receiver may then determine, from the received information, if the containing elements includes the asset.

[0064] The information may be required by the system to execute the conveyance, which may be a consignment sale. The interest may include an ownership interest in the asset. The interest may include a right to use the asset. The circuit may be configured to communicate the information before a third party places the asset in the possession of the second party. The third party may be a vendor, for example without limitation, a retailer, a wholesaler, a rental agent, or any other suitable entity. The third party may be an entity that does not hold an ownership interest in the asset during the conveyance.

[0065] In some embodiments, the invention may provide an asset container that may include a containing element configured to receive and enclose the asset. The containing element and/or the asset may include an electrical circuit configured to communicate information corresponding to the asset to a receiver outside the containing element when the containing element is closed. A circuit deactivator may be configured to interrupt electrical communication within the circuit.

[0066] The deactivator may be configured to interrupt electrical communication between a first

portion of the circuit and a second portion of the circuit. The first portion may include a digital data storage device. The second portion may include an antenna. The deactivator may be configured to interrupt the electrical communication by physically separating the first and second portions of the circuit. The deactivator may be configured to be operated manually by a user of the asset.

[0067] The information may be configured to be used by a benefit denial system to provide to a user access to a benefit. The information may be required by the benefit denial system to provide the access. The information may be configured to be used by an asset transaction system to convey an interest in the asset from an interest conveyor to an interest receiver. The information may be required by the asset transaction system.

[0068] In some embodiments, the invention may provide a method for providing a benefit of an asset to an asset user. The method may include receiving asset identification information transmitted by an antenna enclosed in a containing element and providing access information corresponding to the asset identification information to the user. The access information may be configured to provide the user with access to the benefit.

[0069] The method may include providing the access information to the user via a point-of-sale entity. The method may include notifying a content provider regarding that the user has initiated a purchase of the asset. The content provider may be an entity that owns or possesses or is conveying a copyright, patent right,

trademark right, trade secret, or other right or intellectual property right in the asset.

[0070] The method may include providing a label to the user. The label may bear at least a portion of the access information (such as a PIN). The label may be configured to adhere to the container. The portion may be human-readable or machine readable and may include a barcode, hologram, watermark, or other indicia.

[0071] The asset identification information may include an electronic product code. The asset identification information may include a universal product code.

[0072] The method may include activating the benefit. The activating may include identifying the access information as active access information. The access information may be stored in a storage device and electronically identified as "active."

[0073] The method may include receiving the access information from the user. The method may include providing to the user a key to the benefit if the access information received from the user corresponds to access information identified in the storage device as activated access information. The key may serve to activate the asset. The key may serve to activate the benefit.

[0074] It will be appreciated that, according to the principles of the invention, the terms "active", "activating" and "activated", as applied to access information, refer to the process by which a system (such as a benefit denial system) designates that a benefit corresponding to the access information will be conferred to a user if the user presents the access information (or a facsimile thereof) to the system.

The system may then activate the benefit by providing information required to provide the benefit to the user. If the user presents access information (or a facsimile thereof) that does not correspond to activated access information, system will not activate the benefit and the user will be denied the benefit.

[0075] A number of features of illustrative embodiments of the invention are shown in FIGS. 1-15.

[0076] FIG. 1A shows an illustrative lockable container in accordance with one embodiment of the invention. Container 30 includes a first cover 32, a second cover 34, and a spine 36 disposed therebetween. First cover 32 and second cover 34 are pivotally coupled to spine 36 to form a living hinge.

[0077] Container 30 may include a locking mechanism. The locking mechanism of the invention may be integral with the container, and therefore may remain with the container, regardless of whether the container is locked or unlocked. Thus, the container may be both locked and unlocked without removing any portion of the locking mechanism (e.g., a locking member) from the container. Accordingly, there is no need to reuse, restock, recycle or discard any portion of the locking mechanism.

[0078] Container 30 may be locked to secure an asset within the container. In particular, container 30 may include internal locking member 100 and a locking mate arrangement situated within container 30. Locking member 100 and locking mate arrangement are configured for engagement such that first cover 32 is secured to second cover 34, thereby securing an asset within container 30.

[0079] FIG. 1A shows container 30 with locking member 100 inserted therein in the unlocked position. Locking member 100 may be inserted into container 30 after the container has been manufactured. For example, locking member 100 may be snapped into place within container 30 at the location in which the container is manufactured. As shown in FIG. 1A, in some embodiments of the present invention, at least one end of locking member 100 may be extended to the edge of container 30 to provide more security. This may prevent, for example, a thief from prying at the corners of container 30 to attempt to open the container.

[0080] In some embodiments, locking member 100 may include at least one spring-arm arranged on an end of the locking member that is configured to magnetically couple with an external manual magnetic key arrangement. The spring arm causes locking member 100 to alternately move into the locked and unlocked positions. In the embodiment shown in FIGS. 1B and 1C, and as more fully explained below, locking member 100 may include spring arms 102 and 104 arranged on opposite ends of the locking member.

[0081] In some embodiments of the present invention in which spring arms 102 and 104 are integrally formed (e.g., molded) with locking member 100, the spring arms may need to be rotated out of alignment with the longitudinal axis of locking member 100 so that magnetic inserts 174 and 172 are properly positioned within the spring arms. The process of rotating each of spring arms 102 and 104 out of alignment with locking member 100, however, may cause an unwanted bias on the spring arms, thereby causing locking heads 170

and 168 to be displaced outward in a direction perpendicular to the longitudinal axis of locking member 100. Accordingly, each spring arm 102 and 104 may be provided with hooks 184 and 180, and hook catches 186 and 182, respectively. In this manner, spring arms 102 and 104 may be properly positioned after inserting magnetic inserts 174 and 172, respectively, so that the spring arms do not protrude perpendicularly to the longitudinal axis of locking member 100.

[0082] As shown in FIGS. 1B and 1C, locking member 100 includes multiple I-beam engagement portions for engaging associated tabs or protrusions within container 30. Locking member 100 includes three engagement portions 106, 108, and 110 that will be referred to herein as "single engagement portions." "Single engagement portion" shall refer to an engagement portion that has no corresponding engagement portion on the opposite side of locking member 100. Locking member 100 includes eight engagement portions 112 and 114, 116 and 118, 120 and 122, and 124 and 126 that will be referred to herein as "double engagement portions." "Double engagement portion" shall refer to an engagement portion that has a corresponding engagement portion on the opposite side of locking member 100. (It should be noted that although locking member 100 is described herein as having three single engagement portions and eight double engagement portions, this arrangement is merely illustrative, and locking member 100 may have any suitable arrangement and number of engagement portions.)

[0083] The double engagement portions of locking member 100 (i.e., portions 112-126) are configured to

engage associated tabs of first cover 32 and second cover 34 of container 30. Each engagement portion (i.e., engagement portions 106-126) includes a locking trench and a release trench. The various locking trenches are designed so that when container 30 is closed and the tab portions on first cover 32 are aligned with the corresponding tab portions on second cover 34, locking member 100 slides into the locked position so that each locking trench catches and traps the corresponding tab portions therebetween, preventing the corresponding tab portions from being separated. This alignment prevents container 30 from being opened.

[0084] In particular, engagement portions 106, 108, and 110 each have locking and release trenches 128 and 130, 132 and 134, and 136 and 138, respectively. Engagement portions 112 and 114 include locking trenches 140 and 142, respectively. With regard to release trenches for engagement portions 112 and 114, the engagement portions share a "release trench" 93 in container 30. In actuality, release trench 93 is a space within container 30. Engagement portions 116 and 118 each include locking and release trenches 144 and 146, and 148 and 150, respectively. Engagement portions 120 and 122 each include locking and release trenches 152 and 154, and 156 and 158, respectively. Engagement portions 124 and 126 each include locking and release trenches 160 and 162, and 164 and 166, respectively.

[0085] To lock container 30, locking member 100 is made to slide in a direction that engages the corresponding tabs with the appropriate locking trenches. This traps the corresponding tabs within the locking trenches and prevents the tabs from separating

and, consequently, the container from opening. In other words, the container may not be opened, since the associated tabs of first cover 32 are prevented from freely traversing the various release trenches when the first cover is pulled away from second cover 34.

[0086] Locking member 100 may include status indicator 190 on the face of locking member 100 which may include locking and unlocking status information. The status information may be placed thereon by known method. When the locking member 100 is slid between the locked and unlocked positions, the appropriate status information corresponding to the position of the locking member, for example, may appear through a status window of container 30 for a user to read.

[0087] FIG. 2A shows illustrative information 260 that may be communicated between container 263, which may include antenna 262, and system 268, which may include transceiver 261. System 268 may be associated with a point-of-sale ("POS") system at an asset retail or rental facility. For the purpose of illustration, system 261 will be described as being associated with a retail sales facility. Information 260 may be associated with asset 264. Information 260 may include security information that is required for user 290 to access asset 264 or a portion of asset 264. Information 260 may be required for user 290 to obtain a benefit present on or in asset 264.

[0088] In some embodiments, information 260 may be required to initiate a process that provides user 290 with access information 270 that may enable user 290 to access asset 264 or obtain a benefit present on or in asset 264. In some embodiments, information 260 may be required to initiate a process that provides user 290

with activation information 272 that may activate a benefit present on or in asset 264. For the purpose of illustration, the benefit will be described as the use of an electronic game.

[0089] User 290 may purchase asset 264 and execute the purchase by interacting with system 268. System 268 may receive information 260 using transceiver 261. Information 260 may be transmitted by antenna 262 on a radio frequency carrier signal. In some embodiments, system 268 may transmit sale information 274, which may be derived from or included in information 260, to content provider 282. It will be understood that the functions described herein as being performed by content provider 282 may be performed by any suitable party using one or more of a system for processing data, a system for communicating data, a system for storing data and any other suitable system. The system or systems may be centralized. The system or systems may be distributed over one or more physical deices. The physical devices may be located in different geographic locations.

[0090] System 268 may communicate with content provider 282 via a computer network such as the Internet, a virtual private network or other suitable secure data circuit, or an intranet, via a telephone network, via a wireless communication channel, or via any other suitable communication channel. Sale information 274 may inform content provider 282 that asset 264 has been or is to be sold to user 290 and that the sale occurred through system 268. Content provider 282 may therefore recognize the sale of asset 264 as an authorized or authentic sale. Content provider 282 may provide access information 270 to user

290. In some embodiments, content provider 282 may provide access information 270 to user 290 via system 268. In some embodiments, content provider 282 may provide access information 270 to user 290 via a route (not shown) that is independent of system 268. Access information 270 may be communicated to user 290 via a computer network such as the Internet or an intranet, via a telephone network, via a wireless communication channel, or via any other suitable communication channel.

[0091] System 268 may provide access information 270, which may be derived from or be included in information 260, to user 290. User 290 may use access information 270 in conjunction with access device 265 to access or play a computer game stored on asset 264. Access device 265 may be an access device such as any of those described above. It will be assumed for the sake of illustration that the access device is an electronic game system.

[0092] In some embodiments, user 290 may "keyboard" access information 270 into access device 265. Access device 265 may communicate access information 270 to content provider 282. Content provider 282 may identify access information 270 as being authorized access information and may provide activation information 272 to user 290, for example via access device 265. Communication between content provider 282 and access device 265 may be via a computer network such as the Internet or an intranet, via a telephone network, via a wireless communication channel, or via any other suitable communication channel.

[0093] In some embodiments of the invention, asset 264 may instruct access device 265 to communicate

with content provider 282. Asset 264 may include a log-in procedure that prevents access device 265 from launching the computer game until access device receives activation information 272. Access device 265 may display a screen that prompts user 290 to enter some or all of access information 270 into access device 265. After access device 265 receives activation information 272, access device 265 may launch the electronic game. User 290 may then obtain the benefit of playing the electronic game.

[0094] In some embodiments, information 260 may include activation information 272 that is provided to user 290 by system 268. In those embodiments, it may not be necessary for system 268 to provide sale information 274 to content provider 282, for content provider 282 to provide access information 270 to user 290, or for access device 265 to communicate with content provider 282. In some of those embodiments, user 290 may keyboard access information into access device 265. Asset 264 may instruct access device 265 to launch the electronic game upon receipt by access device 265 of the activation information.

[0095] In some embodiments of the invention, access device 265 may be provided with a transceiver that is configured to communicate directly with antenna 262. In those embodiments, user 290 may place container 263 in communication with access device 265 to transfer any portion of information 260 required for access to asset 264, or a benefit present in or on asset 264, to access device 265.

[0096] In some embodiments of the invention, access device 265 may not be in communication with content provider 282. For example, access device 265 may not

have an Internet interface. User 290 may communicate with content provider 282 by telephone. User 290 may provide access information 270 to content provider 282 via telephone. Content provider 282 may provide activation information 272 to user 290. User 290 may enter activation information 272 into access device 265 to gain access to the electronic game.

[0097] In some embodiments of the invention, information 260 may be used to execute a consignment sale of asset 264. The consignment sale may be a transaction between content provider 282 and user 290. The sale may be facilitated by system 268. The retail sales facility may not own asset 264. The retail sales facility may own asset 264, but may not own the computer game stored on asset 264. Therefore, if asset 264 is lost or stolen, the retail sales facility may lose the value of asset 264 in its inactive state, but may be spared the loss of the electronic game value.

[0098] System 268 may provide consignment sale information 276 to content provider 282. Consignment sale information 276 may inform content provider 282 that user 290 has purchased or has agreed to purchase asset 264 and the computer game present on asset 264. Content provider may provide access information to user 290 to enable user 290 to play the electronic game, as described above. User 290 may provide funds 280 to the retail sales facility associated with system 268. User 290 may provide funds 280 to content provider 282 via financial institution 284. System 268 may facility the transfer of funds 280 by providing transaction information 278, which may be credit card information, to financial institution 284. Any of the

aforementioned communications in connection with the consignment sale may be performed via a computer network such as the Internet or an intranet, via a telephone network, via a wireless communication channel, or via any other suitable communication channel.

[0099] It will be understood that in some embodiments of the invention, information 260 may include security information that is required for user 290 to access asset 264 or a portion of asset 264. In some embodiments, information 260 may include information that may be used to execute a consignment sale of asset 264. In some embodiments, information 260 may include both security information that is required for user 290 to access asset 264, or a portion of asset 264, and information that may be used to execute a consignment sale of asset 264.

[0100] FIG. 2B is a schematic diagram showing illustrative communication system 200 in accordance with one embodiment of the invention. Lockable container 202 may be any suitable containing element, including the lockable containers described in U.S. Patent Publication No. 2004/0129587, 2002/0023853, 2003/0000856, 2003/0111367, and 2004/0129587. Lockable container 202 may include one or both of RFID tag 206 and optical tag 208. RFID tag 206 and optical tag 208 may be disposed on the exterior surface of container 202, within container 202, and/or on asset 204 held within container 202. Asset 204 may be secured inside lockable container 202. In some embodiments, lockable container 202 contains a disc hub for securing a CD, DVD, or other similar disc.

[0101] RFID tag 206 maybe passive or active. In some embodiments, if RFID tag 206 is an active tag, then a battery may power the tag. RFID tag 206 may also be read-only or read-writable. RFID tag 206 may transmit item identification data (or any other suitable information) to decoupler 210 continuously or after being interrogated by a component of decoupler 210. Similarly, decoupler 210 may transmit data to RFID tag 206. Although for the sake of clarity only one instance of RFID tag 206 is shown in FIG. 2, any number of tags may be located on lockable container 202 or on asset 204. In some embodiments, lockable container 202 also contains at least one optical tag 208. Optical tag 208 may include, for example, a barcode, watermark, machine-readable indicia, or any other optical tag conveniently positioned on lockable container 202 or asset 204.

[0102] Lockable container 202 may also include at least one reflective tag 205. Reflective tag 205 may be configured to move between a first position and a second position. In the first position, reflective tag 205 may close an optical circuit between the tag and an optical sensor. In the second position, reflective tag 205 may open an optical circuit between the tag and the optical sensor, such as optical sensor 214. The tag may include at least two portions of different reflectivity. In some embodiments, reflective tag 205 comprises reflective foil or tape and indicates whether lockable container 202 is locked or unlocked. In other embodiments, reflective tag 205 includes indicia printed or treated with reflective ink or other reflective material.

[0103] Reflective tag 205 may be configured to move or change orientations within lockable container 202 based on the security status of lockable container 202. In at least one embodiment, reflective tag 205 is attached to a locking member of lockable container 202. The locking member may be internal to lockable container 202 and may have a locked position and an unlocked position. The locking member may be moved between the locked and unlocked positions by a magnetic force. As described in more detail in FIGS. 11A and 11B below, reflective tag 205 may be moved along with the locking member, so that tag 205 is indicative of the security status of lockable container 202. One portion of reflective tag 205 having another reflectivity may indicate that lockable container 202 is locked, while another portion of reflective tag 205 having a different reflectivity may indicate that lockable container 202 is unlocked. Reflective tag 205 may be configured to reflect electromagnetic radiation at varying intensities or in different wavelengths (e.g., color of visible light).

[0104] Lockable container 202 may be received by decoupler 210. The term "decoupler" or "automatic container processing assembly" is meant to refer to any device or apparatus capable of accepting, engaging, and/or processing asset containers. In some embodiments, these asset containers may be lockable containers as described above. The decoupler or automatic processing assembly may mechanically perform at least one processing task typically performed by a retail clerk. These tasks may include, for example, locking or unlocking the container, scanning an optical tag associated with the container, or any other

suitable task. Before or after being received by decoupler 210, RFID tag 206 may transmit to, or receive data from, RFID transceiver 212 of decoupler 210. In some embodiments, lockable container 202 may be inserted into processing path 216. In some embodiments, processing path 216 may engage lockable container 202.

[0105] At least a portion of processing path 216 may be exposed to or overlay a magnetic field. The magnetic field may be created by a magnetic field source, such as one or more electromagnets. The magnetic field source may be switched on and off while lockable container 202 is in processing path 216. The magnetic field may selectively lock or unlock lockable container 202 as container 202 is moved through processing path 216. Container 202 may also pass optical sensor 214. Optical sensor 214 may determine the position or orientation of reflective tag 205 by detecting electromagnetic radiation reflected from reflective tag 205. In some embodiments, optical sensor 214 may detect reflected visible light intensity. In some embodiments, optical sensor 214 may detect the color of the reflected visible light. Optical sensor 214 may include a light source, such as a light emitting diode ("LED") or laser. Lockable container 202 may be aligned with the light source via a motorized conveyor or transport assembly, as described in FIG. 3 below. Optical sensor 214 may also include an optical scanner, such as a barcode scanner, for reading optical tag 208 on lockable container 202. Optical tag 208 may be read before, after, or while the container is being processed by decoupler 210.

[0106] In addition to receiving lockable container 202, decoupler 210 may, in some embodiments, also eject the container along the same processing path that the container was received. For example, a consumer who wishes to rent a DVD movie may insert the DVD container into decoupler 210. The DVD container may be processed by decoupler 210 moving the container along processing path 216. The container may be ejected from decoupler 210 after processing is complete and returned to the consumer. In some embodiments, the container is not returned to the consumer, but rather moved straight through the decoupler to the back side of decoupler 210. This embodiment may be useful in rental return situations where the asset is being returned to inventory. This embodiment may also reduce theft of assets dropped in an overnight drop box. Decoupler 210 may be connected to another processing device, such as a mechanical conveyor, robotics, or belt system for further processing, or an inventory bin may be positioned at the back side of decoupler 210.

[0107] Decoupler 210 may perform one or more of several actions after lockable container 202 is received by decoupler 210. The sequence of actions taken by decoupler 210 may depend on one or more of several criteria, including, but not limited to, the security status of lockable container 202 (e.g., locked or unlocked), the processing status of the asset in the lockable container 202 (e.g., rented and/or purchased), information received from RFID tag 206 (either on the container, on the asset, or both), and information received from optical tag 208.

[0108] Decoupler 210 may be multi-functional. Decoupler 210 may scan optical tag 206 while processing

the asset. Decoupler 210 may also interpret an information signal emitted from the asset or the container via RFID tag 206. If the signal validates the asset, decoupler 210 may act in response to the signal. To validate the asset, decoupler 210 may communicate with transaction management facility 220. Transaction management facility 220 may include any host, server, data source, or database containing asset or container information. Transaction management facility 220 may also coordinate communication between one or more of decoupler 210 and content provider 230, asset management module 240, financial instructions 250, and any other suitable device or entity.

[0109] To validate an asset, asset identity information may be received from lockable container 202 and/or asset 204 via one or more of RFID tag 206, optical tag 208, and reflective tag 205. This received information may be compared against information accessible by transaction management facility 220. Transaction management facility 220 may also communicate with content provider 230, asset management module 240, and/or financial institutions 250 to complete the validation process. For example, transaction management facility 220 may notify asset management module 240 to deactivate a security tag associated with the item so that an alarm will not sound when the item is passed through sensors located at the exit of the store, library, or other location. As another example, transaction management facility 220 may automatically debit the purchase or rental price of the asset from the consumers account by contacting financial institution 250. Transaction management facility 220 may also access information relating to

the processing status or availability of the asset in lockable container 202. For example, the item may be sold out or not available for rental. As another example, the processing status may indicate that the asset in the lockable container is for sale only and not for rental. Transaction management facility 220 may access content provider 230 for network access, security information, or media content. In some embodiments, decoupler 210 may write, burn, or record media content or other data from content provider 230 directly to asset 204 or RFID tag 206 while processing the asset.

[0110] If the transaction is validated, decoupler 210 may act on lockable container 210 in accordance with a processing sequence based on the received information. The acting may include, among other actions, transporting the asset along processing path 216, locking or unlocking the container, scanning optical tag 208, writing security information or other data to RFID tag 206, verifying the status of the container after processing, and releasing the container.

[0111] In some embodiments, decoupler 210 may process lockable container 202 in stages. The first stage of processing may include an interpretation stage, in which information emitted from the asset or the container is received and analyzed. The second stage of processing may include a transport stage, in which the container is moved within decoupler 210 along processing path 216. The third stage of processing may include an acting stage, in which the decoupler acts (e.g., engages the container and/or moves the container along processing path 216) on information received from

the container or the asset. The final stage of processing may include an ejection stage, in which the decoupler releases the container or positions the container such that it may be removed from the decoupler by a user or another device.

[0112] The decoupler may be configured to receive and release the container to an individual or to another device. In some embodiments, the container is released to the consumer along the same processing path as the container was received. In other embodiments, the container is released along a different processing path than the processing path that container was received.

[0113] During the decoupler transport stage, the container may be conveyed to a "read" position. In the "read" position, the decoupler may receive information from, or transmit information to, the asset or the container. The apparatus may include one or more motorized belts. The apparatus may move the container into or through a magnetic field generated by one or more magnets. One or more of the magnets may be permanent magnets or electromagnets. One or more of the magnets may be in a fixed location within decoupler 210. Passing the container into or through the magnetic field may lock and/or unlock the container. In some embodiments, the container may be first locked during the transport stage and then locked or unlocked during the acting stage.

[0114] During the decoupler acting stage, the decoupler may take one or more actions in response to the information received from the interpretation stage. The actions may include one or more of reading RFID tag 206, writing to RFID tag 206, killing (deactivating)

RFID tag 206, activating an EAS tag, deactivating an EAS tag, unlocking the container, locking the container, or any other suitable action. Table 1 summarizes some of the exemplary actions the decoupler may take based on the security status of the container and the processing status of the asset in the container.

Table 1 - Exemplary decoupler actions.

Security Status	Processing Status	Exemplary Decoupler Action(s)
Secured	For Sale	Receive information; relock container; scan optical tag; activate product; unlock container; and verify unlocked status.
Not Secured		Lock container; receive information; scan optical tag; activate product; unlock container; and verify unlocked status.
Secured	For Rent/ For Loan	Receive information; relock container; scan optical tag; activate product; unlock container; and verify unlocked status.
Not Secured		Lock container; receive information; scan optical tag; activate product; unlock container; and verify unlocked status.
Secured	For Return	Receive information; relock container; scan optical tag; deactivate product; and verify locked status.
Not Secured		Receive information; lock container; scan optical tag; deactivate product; and verify locked status.

[0115] Table 1 is merely illustrative. The decoupler may be configured to perform any other suitable actions to automate the checkout or return

process. In addition, the order of the operations listed above are exemplary. The above actions may be performed, or combined, in any suitable manner. For example, when returning an unsecured asset in a lockable container, the decoupler may first lock the container and then receive status information from the container and/or the asset. In addition, in some embodiments information may be received from both the container and the asset in the container. This information may be used to verify the presence of the asset in the container. For example, if a rental consumer tries to return a lockable DVD container without the correct DVD asset inside the container, the decoupler may reject the container. In other embodiment, the decoupler may process the container, but not alter the processing status information associated with the item.

[0116] In order to determine that the container was unlocked properly or in an authorized manner, optical sensor 214 may verify the security status of the container while the container is still in the decoupler. The sensor may read reflected electromagnetic radiation, which may include in some emboidments visible light, from reflective tag 205. Reflective tag 205 may be indicative of the security status of the lockable container. In some embodiments, reflective tag 205 may have a color or be configured to reflect light of a certain color or wavelength. The tag may be positioned on a locking portion (such as a locking bar) of the lockable container so that when the container is locked and unlocked, the orientation of reflective tag 205 may change. In some embodiments, reflective tag 205 includes a colored "unlocked" icon

treated with a reflective ink (the color of the ink may be green). In these embodiments, optical sensor 214 may detect both intensity and color of the electromagnetic radiation. In other embodiments, optical sensor 214 may detect only electromagnetic radiation intensity and not color. Reflective tag 205 may be disposed at at least two positions, a reflective position, in which tag 205 closes an optical or opto-electrical circuit between tag 205 and the optical sensor, and a non-reflective position, in which tag 205 opens the optical circuit between the tag and the optical sensor. Optical sensor 214 may optically sense or confirm the position or orientation of reflective tag 205 to confirm the security status of the container.

[0117] In some embodiments of the invention, decoupler 210 may be configured to activate the asset in lockable container 202 (as in a checkout activation system). In some of these embodiments, decoupler 210 may enable authorized access to digital media. The decoupler may provide an activating ingredient or excitation to the asset that changes the potency of the substance--for example, a pharmaceutical product--in order to activate a property, which may be a therapeutic property, of the substance. In other embodiments, decoupler 210 includes a transmitter, which may be an RF transmitter, for sending security information to RFID tag 206 or some other storage or memory mechanism associated with the lockable container or the asset within the lockable container.

[0118] Decoupler 210 may be configured to automatically process purchases, rentals, returns, and any other consumer transaction. For example, a user

may selects an asset displayed "live" on a shelf in a lockable container. The lockable container may show a red "locked" icon indicating that a locking bar in the container is in the locked position. The user may insert the container into decoupler 210 in a specific orientation. In one embodiment, the user inserts the container oriented with the locked icon on right side, hinge on left side. The decoupler may then engage the lockable container with a container transport assembly and move the container along a processing path. The processing path may expose at least a portion of the container to a magnetic field. The magnetic field may be used to lock or unlock a magnetically actuated locking member of the container. The decoupler may also perform any of the processing actions described above while moving the container along the processing path. At the conclusion of the processing stage, the decoupler may alter the processing and/or security status of the container, as appropriate. For example, after a rental CD has been rented, the decoupler may alter the CD's processing status to "unlocked-rented" or some other similar status.

[0119] FIG. 3 shows a schematic diagram of a top view of an illustrate transport chassis of the decoupler of FIG. 2. Transport chassis 312 may be secured to main chassis 300. Main chassis 300 is described in more detail below in connection with FIG. 5. Transport chassis 312 may include LED signals 306. LED signals 306 may indicate the processing stage of the decoupler. For example, in one embodiment LED signals 306 include a red and green LED. The green LED may indicate that the decoupler is online and powered. The red LED may indicate that the decoupler is

currently processing a container, such as container 310. When processing has finished, the red LED may turn off, signaling to the user that processing is complete. The user may then remove container 310 from transport chassis 312. If the container could not be processed (e.g., an optical tag or RFID tag associated with the container could not be read and/or written to), LED signals 306 may flash indicating an error condition.

[0120] Once a container is positioned within the RFID or optical field of the decoupler, the decoupler may read from, write to, or kill one or more RFID tags associated with container 310 and/or an asset within container 310. If the decoupler determines that the information received from the one or more RFID tags constitutes a valid transaction, the decoupler may activate conveyor assembly 308. Alternatively or additionally, when optical sensor 304 scans, detects, or recognizes a valid optical tag on container 310, the decoupler may activate conveyor assembly 308. Optical sensor 304 may include any switch, sensor, or scanner, including a position sensor, that detects or reads machine-readable information from container 310. After container 310 is detected in transport chassis 312, the container may be transported to the back of transport chassis 312. Conveyor assembly 308 may be a powered or unpowered assembly. In one embodiment, a user may manually pushes container 310 into transport chassis 312. The user's force may move conveyor assembly 308, resulting in the mechanical energy needed to power the remainder of the decoupler. In other embodiments, the decoupler may be powered via an external power source. The external power source may be used to create an

electromagnetic drive system with reversible polarity. The electromagnetic drive system may be used to effect movement of metal reaction portions of the lockable container causing the container to lock or unlock. Optical sensor 304 may cause an electrical signal to be transmitted to a motor attached to conveyor assembly 308. This electrical signal may cause conveyor assembly 308 to transport container 310 further into transport chassis 312.

[0121] In some embodiments, transport chassis 312 may accept variable-sized containers. For example, conveyor assembly 308 may be supported by springs (not shown), which dynamically adjust to fit the size of the container to be processed. Conveyor assembly 308 may also include any number of sprockets, wheels, and/or conveyor belts. In the depicted embodiment, one endless belt is shown; however, any number of belts and any number of conveyor assemblies may be used in other embodiments.

[0122] Optical sensor 304 may also scan container 310 as it moves into transport chassis 312. For example, optical sensor 304 may scan a portion of the container containing a barcode, watermark, hologram, or any other machine-readable indicia. In some embodiments, conveyor assembly 308 may stop the transport of container 310 so that optical sensor 304 may scan a tag associated with container 310. In other embodiments, the container is scanned while being transported to the back of transport chassis 312.

[0123] At some point, container 310 may make contact with rear contact switch 314, which may be located at the back of the processing path of the decoupler. Rear contact switch 314 may include any switch or sensor,

including a position sensor. Once contact switch 314 is actuated, conveyor assembly 308 may reverse the container's direction of motion. Although in the example of FIG. 3 container 310 may be transported back along the same physical processing path from which it entered, in other embodiments container 310 may be transported along a different physical processing path. For example, container 310 may be transported straight through the decoupler in some embodiments. Thus, a user may insert container 310 in one of side of the decoupler, and the container may be released, or ejected, on the other side. One or both sides of the decoupler may be connected to another device or apparatus that handles the processed container. For example, a conveyor belt may be connected to the decoupler to take the output containers back to a warehouse or other storage facility. As another example, a device (such as a conveyor) may automatically feed containers into the decoupler for processing, if desired.

[0124] Transport chassis 312 may expose container 310 to one or more magnetic forces. These magnetic forces may result from a magnetic source within the decoupler or one or more external magnetic sources. For example, in one embodiment the decoupler contains magnets 604 (FIG. 6) conveniently positioned within the processing path of container 310. These electromagnets may activate or deactivate a security tag, such as an EAS tag, lock the container, unlock the container, or perform any other suitable action (e.g., completely or partially wipe a magnetic storage medium associated with container 310). For example, container 310 may be associated with a benefit denial device. In order for

the asset in container 310 to provide a benefit to the user, security or product activation information must be written to a device associated with the asset. Upon processing container 310, the decoupler may automatically blank or erase a magnetic storage medium containing such security or activation information and rewrite the information as appropriate. The magnetic field may be used for other processing actions as well. For example, container 310 may include an internal locking member which is configured to be moved by a magnetic force between a locked position and an unlocked position. By exposing container 310 to an appropriately oriented magnetic field, the decoupler may lock or unlock container 310. In some embodiments, containers are always locked upon entering transport chassis 312 and then locked or unlocked depending on the particular processing sequence executed by the decoupler.

[0125] Optical sensor 304 may verify or confirm the processing or security status of container 310 at any convenient time. For example, in one embodiment before the decoupler ejects container 310, optical sensor 304 attempts to verify the container's security status. In some embodiments, optical sensor 304 may detect electromagnetic radiation reflected off reflective tag 205 (FIG. 2). This radiation may be include infrared ("IR"), ultra-violet ("UV"), visible light, or any other suitable frequency of electromagnetic radiation. Container 310 may include a portion configured to close an optical or opto-electrical circuit with optical sensor 304 in one position while opening the optical circuit in another position. In some embodiments, optical sensor 304 detects the intensity of reflected

radiation only. In other embodiments, optical sensor 304 detects the intensity and/or the frequency of reflected radiation (e.g., the color of reflected visible light). The position of the portion of container 310 that reflects the radiation may be indicative of the security status of container 310. This security status may indicate that container 310 is locked or unlocked.

[0126] During movement of container 310, an EAS tag may be deactivated, a barcode or other optical tag may be optically scanned, and/or one or more RFID tags may be read, written to, or killed. When container 310 enters the RFID or optical field of the decoupler, the decoupler may interrogate the container and/or the asset in the container to authenticate a valid transaction. For example, in one embodiment, passive RFID tags associated with the asset and the container are interrogated. The decoupler may verify whether the correct asset is in the correct container and validate the transaction using any other available information from transaction management facility 220 (FIG. 2). If the transaction is confirmed, the decoupler may energize conveyor assembly 308 and accept container 310. The decoupler may then release a solenoid arm, which may block the container's processing path, to allow case to advance into decoupler assembly.

[0127] Once in the assembly, a magnetic field may lock a locking bar internal to container 310. The container may then be moved to rear contact switch 314, which signals a motor to reverse direction of conveyor assembly 308. At this point, container 310 may begin to exit the transport chassis. The container's locking bar is again affected by a magnetic field, which may

unlock container 310. Container 310 may then show a green "unlocked" icon in a lock indicator window on the container. When the lock indicator window passes optical sensor 304, electromagnetic radiation may be reflected from a portion of container 310 and detected by optical sensor 304. LED signals 306 may then flash to indicate successful unlocking of container 310. In some embodiments, other suitable output devices or mechanisms are used to indicate the successful unlocking of container 310. For example, a display screen or speaker may be integrated into the decoupler to allow multimedia output as well as user input.

[0128] Finally, when container 310 passes contact switch 302, conveyor assembly 308 may discontinue moving the container. Contact switch 304, like rear contact switch 314, may include any switch, sensor, or scanner, including a position sensor, that detects or reads the position of container 310. Once the processing of the container is complete and the container is ejected from the processing path, the user may remove the processed container from the decoupler.

[0129] In rental store and library environments, products rented or borrowed must be returned. In order to help speed the process of returning these items, a coupling embodiment of the invention may be used. In these embodiments, a container may pass all the way through the decoupler, locking the case and the media inside while receiving asset return information, which may include inventory information. This embodiment may be used in any type of stocking situation where individual assets are scanned for inventory, such as in the video rental industry, the library system and the pharmaceutical industry (for example, a retail pharmacy

may stock a drug or other item by scanning a container, writing information to an RFID tag on the container, and locking the container, thus securing the drug or other item inside). The coupling embodiment may transport a container with an asset, receive information from the asset or from the container, and act upon the information. The decoupler may process the asset in a number of ways, including, for example, reading from, writing to, or killing one or more RFID tags associated with the asset and/or the lockable container, activating or deactivating an EAS tag associated with the asset and/or the lockable container, and locking or unlocking the container. In addition, the decoupler may connect to network resources, such as inventory information, asset management information, or stored data to further process or validate the asset.

[0130] A user may return a rental or retail item in a lockable container showing a green "unlocked" icon. This icon may indicate that the locking bar in the container is in the unlocked position. The user may insert the container into the decoupler in the appropriate orientation. In one embodiment, the user inserts the container with the indicator on the right side of the container with the container spine on left.

[0131] Information reception and/or transmission may begin when, for example, the container enters the RFID reader or optical field of the decoupler. This may cause conveyor assembly 308 to begin transporting the container. While in transport, an EAS tag may be activated, a barcode may be optically scanned, and/or an RFID tag may be read, written to, or killed. At some point, container 310 may trigger a contact switch,

which recognizes the position of the container and interrogates a passive RFID tag associated with the container and/or the asset in the container to authenticate the transaction and to credit its return to the user. Authenticating the transaction may include matching the asset with container 310 and/or connecting to stored data or transaction management facility 220 (FIG. 2) to determine that the container is eligible for processing.

[0132] If the transaction is authenticated, the decoupler may energize conveyor assembly 308 and release a solenoid arm, which blocks the processing path, to allow the container to advance straight through the clear processing path. The container may be exposed to one or more magnetic forces, causing the locking bar within the container to be affected, which may lock the container. The container then is transported out the rear of the decoupler. Optionally, a storage bin may hold processed containers at the rear of the decoupler.

[0133] FIG. 4 shows a bottom view of the illustrative transport chassis of FIG. 3 in accordance with one embodiment of the invention. Transport chassis 400 may include one or more magnets 406. In some embodiments, magnets 406 are permanent magnets. In other embodiments, magnets 406 are electromagnets. Magnets 406 are positioned in such a way so as to create a magnetic force configured to lock and/or unlock container 410 as it is transported through transport chassis 400. Magnets 406 may be switched on and off at appropriate times via electric current.

[0134] Magnet cover 408 may protect or shield other circuitry in the decoupler from being exposed to the

magnetic field created by magnets 406. Antenna 402 may be any suitable device which receives or radiates radio waves, including RF waves. Antenna 402 may be combined or connected to RFID transceiver 506 (FIG. 5) to form an RFID reader. Motor 404, which may be connected to a power source (not shown), may power the container transport assembly.

[0135] FIG. 5 shows a top view of an illustrative main chassis. Programmable logic controller 518 may coordinate some or all of the decoupler actions. For example, programmable logic controller 518 may control the operation of motor 512, micro relay board 514, RFID transceiver 506, and LED signals 504, in order to effect various decoupler processing actions. Power terminal 508 may provide external electrical power to transformer 502, which may then power motor 512, micro relay board 514, programmable logic controller 518, and various other decoupler components. Fuse 510 may protect the decoupler components from electrical surges from power terminal 508 and may be replaceable. Terminal blocks 516 may separate transformer 502 from micro relay board 514 and programmable logic controller 518 to reduce unwanted electrical or magnetic interference. Components shown in FIG. 5 may be shielded, if suitable, to avoid electromagnetic interference.

[0136] FIG. 6 shows an illustrative decoupler assembly. The decoupler assembly may include transport chassis 602 and main chassis 600. In some embodiments, container 614 may be inserted into transport chassis 602 to begin the processing sequence. In other embodiments, container 614 is brought within the RFID or optical range of the assembly to begin the

processing sequence. The top of transport chassis 602 may include flip cover 612 to simplify access to internal components. Flip cover 612 may include magnet cover 610, which may allow access to magnets 604. Thus, magnets 604 may be replaced by removing magnet cover 610. Top cover 606 may be connected to flip cover 612 and may also be pivoted up to allow access to various components of the decoupler.

[0137] FIG. 7 shows a bottom view of illustrative flip cover 700. Hinge pin 704 allows flip cover 700 to pivot about the pin. This allows access to the decoupler components under flip cover 700. In some embodiments, top cover 702 may also pivot about hinge pin 704. In other embodiments top cover 702 is fixed and not configured to pivot. Solenoid 708 may be positioned in flip cover 700 and may be connected to an arm or stop bar 706 that prevents access all the way into the container processing path. In some embodiments, stop bar 706 may selectively impede the processing passageway. In these embodiments, stop bar 706 may be released and removed from the processing path by solenoid 708 based on several factors, including the processing status of the container, the presence of an authenticated container within RFID or optical field range, or any other suitable factor.

[0138] FIG. 8 shows illustrative container 800 for use with the decoupler assembly of FIG. 3. Container 800 may comprise a DVD or CD container. Container 800 includes a first cover and a second cover joined at a spine. The first and second covers may include a plurality of loops that interact with locking member 804 to lock container 800 in the closed position. Locking member 804 is inserted into

container 800 so that it is capable of sliding in directions 818 and 816 into the locked and unlocked positions, respectively.

[0139] Locking member 804 may include molded spring arms 806 and 808 which are, as is more fully described in U.S. Patent Application Publication No. 2004/0129587, used to prevent locking member 804 from sliding into the unlocked position when locked and into the locked position when unlocked. It should be noted that spring arms 806 and 808 may take on any other suitable arrangements so long as they meet the objectives of the present invention. For example, for locking member 804, molded spring arms 806 and 808 may be metal leaf springs (not shown) that are included as part of the second cover of container 800, rather than as part of locking member 804.

[0140] Locking member 804 includes locking tabs 810, 812, 814, and 816 that interlock with adjacent corresponding loops formed on the other cover of container 800 to lock the container in the closed position. Various loops may be disposed on the first cover and the second of container 800. FIG. 8 is intended to show one illustrative arrangement. The loops may be disposed on the second cover of container 800 so that when container 800 is in the closed position, the loops from both covers sit in an adjacent relationship. Locking tabs 810, 812, 814, and 816 are constructed and arranged to at least partially sit within the corresponding loops when locking member 804 is in the unlocked position. This allows the locking tabs of locking member 804 to more easily slide into engagement with the loops of container 800 when the container is in the closed position.

[0141] Locking member 804 is designed to be used with the decoupler of the present invention or an external manual magnetic key decoupler. Either of these devices may selectively lock and/or unlock container 800. In particular, a manual magnetic key decoupler or the decoupler assembly of FIG. 3 may selectively position internal locking member 804 into either the locked position or the unlocked position. For this purpose, internal locking member 804 may include magnetically attractable portions formed therein for magnetically coupling to at least one magnet arrangement of the magnetic key or decoupler. For example, metallic inserts may be inserted at opposite ends of locking member 804, and metallic inserts may be inserted into spring arms 806 and 808.

[0142] The locking member of container 800 may be used with a container for securing assets. Such assets may include, for example, storage media (e.g., DVDs, CDs, video games, memory cards or any other suitable storage media), jewelry, pharmaceutical products, razor blades, printer cartridges, or any other item of value. The lockable container of the present invention may also be used to secure items such that others are prevented from accessing the item, whether or not the item is of particular value. For example, the lockable container of the present invention may be used to secure violent or adult movies or video games in the home, such that children are unable to access the items.

[0143] Container 800 may also include RFID 802 on one or both of the first cover and the second cover. RFID tag 802 may be an active or passive tag. RFID tag 802 may also be disposed at various other locations on

container 800, including, for example, on locking member 804, the container spine, or on the disc hub of container 800. In addition, in some embodiments, RFID tag 802 may be also located on the asset held with the container. For example, a DVD movie may have an RFID tag on the labeled surface of the DVD. This may be useful for verifying the presence of the asset in the container before processing the container. The decoupler of the present invention may read from, write to, or kill any of the aforementioned tags.

[0144] Container 800 may also induce optical tag 801, which in the illustrated embodiments is a barcode, but could include any machine-readable tag or indicia. For example, optical tag 801 may be a hologram, watermark, two-dimensional barcode, or any other printed, etched, or applied tag.

[0145] FIG. 9 shows another illustrative container for use with the decoupler of FIG. 3 in accordance with one embodiment of the invention. Container 900 may include one or more features shown in FIG. 8 in connection with container 800. Some embodiments of the decoupler may accept variable-sized containers. In some embodiments, the containers are a fixed width. For example, container 900 may be a traditional CD jewel case that has the same width as container 800 (FIG. 8). In some embodiments, the decoupler may accept variable-width containers. In these embodiments, the processing path may sense the size of the container and adjust the processing path according.

[0146] Container 900 may include one or more of RFID tag 902 and optical tag 901. RFID tag 902 may also be disposed at various other locations on container 900, including, for example, on locking member 904, the

container spine, or in disc area 904. Container 900 may be configured to hold an asset, such as a CD, DVD, or other like media.

[0147] As shown in FIGS. 10A and 10B, a security status indicator may be displayed through status windows, such as windows 1004 and 1112 on the lockable container. The security status indicator may be indicative of the security status of the container. For example, status portion 1002 may indicate that the locking member is in the locked position. In this position, the lockable container may be locked in the closed position, preventing access to the asset within the container. The status information may be placed on status portion 1002 by any known method. When the locking member of the container is slid between the locked and unlocked positions, the appropriate status information corresponding to the position of the locking member, for example, may appear through status windows 1004 and 1112 for a user to read. In one example, status portion 1002 may include a sticker that shows lock 1006. In some embodiments, lock 1006 is red in color. When the locking member of the container is moved to the unlocked position, status portion 1008 may show opened lock 1110 through status window 1112. In some embodiments, opened lock 1110 is green in color. In one embodiment, at least a portion of status portion 1002 and/or status portion 1008 is treated with reflective ink. In this embodiment, incident light on the status portion may be reflected at the same or different wavelength. For example, incident visible light may be reflected as green light when the locking member is in the unlocked position, while incident

visible light may be reflected as red light when the locking member is in the locked position.

[0148] FIGS. 11A and 11B show illustrative reflective status portions 1104 and 1108 through status windows 1104 and 1110, respectively. Status portion 1102 may contain a reflective icon, such as locked icon 1106, and may indicate the security status of the container. When the container is unlocked (e.g., when the locking member is moved to the unlocked position), status portion 1108 may include a security status indicator configured to close an optical circuit between the indicator and an optical sensor. For example, status portion 1108 may include a reflective foil, reflective film, reflective tape, or other suitable material with a desired (or known) reflectivity. In one embodiment, status portion 1108 may reflect all incident electromagnetic radiation in a portion of the electromagnetic spectrum to an optical sensor, thereby closing an optical or opto-electrical circuit. In other embodiments, status portion 1108 may reflect electromagnetic radiation of a certain wavelength or range of wavelengths only. For example, status portion 1108 may reflect only visible green light when the unlocked security status indicator is showing and reflect only visible red light when the locked security status indicator is showing. The status indicators of FIGS. 11A and 11B are merely exemplary. Any other status indicator capable of being detected, scanned, or read by an optical sensor may be used in place of the depicted status indicators.

[0149] FIG. 12 shows illustrative process 1200 for processing an item in accordance with one embodiment of the invention. At step 1202, the decoupler may engage

the lockable container. Typically, a transfer or transport assembly, such as conveyor assembly 308 of FIG. 3, engages the container. At step 1204, the decoupler receives status information from at least one of the container and the item within the container. For example, RFID tags located on both the container and the item could be interrogated when the container is brought within RFID range of the decoupler. As another example, status information from an optical tag could be scanned, read, or otherwise recognized by an optical scanner or sensor at step 1204. At decision block 1206, via the received status information. The decoupler may connect to any available network resource, server, or content provider to authenticate the transaction. At this stage, the decoupler may link to price information, customer data, and any other related purchase or rental information. For example, if the decoupler recognized the container as a valid container and the asset as a valid asset, the decoupler may transport the container at step 1208. The transport sequence may be based on the received status information from step 1204. Step 1208 may include moving the container along a processing path and altering the status information associated with the container and/or the asset. After the item is transported at stage 1208 or if the transaction status could not be validated at decision block 1206, the illustrative process may stop at step 1210.

[0150] In practice, one or more steps shown in process 1200 may be combined with other steps, performed in any suitable order, performed in parallel -- e.g., simultaneously or substantially simultaneously -- or deleted. For example, step 1204 of receviing

status information may be perfomed before engaging the container at step 1202. For example, when the container enters optical or RFID range of the decoupler, the decoupler may receive information from the container and/or the asset within the container.

[0151] FIG. 13 shows illustrative process 1300 for verifying the security status of a lockable container in accordance with one embodiment of the invention. At step 1302, a security status indicator associated with the lockable container may be aligned with an electromagnetic radiation source, such as a visible light source. At step 1304, the indicator may be exposed to the radiation source. At step 1306, a sensor or some other detector may detect the reflected radiation from the security status indicator. The security status indicator may include a first position that closes an optical circuit between the indicator and the sensor and a second position that opens the optical circuit. If the optical circuit is closed at decision block 1308, this may indicate to the decoupler that the container has been successfully processed and unlocked. The security status of the container is thus verified at step 1312. If the optical circuit is open at decision block 1308, in some embodiments the decoupler may attempt to reprocess the container at step 1310. At this step, the container may be transported through at least a portion of the processing path and once again aligned with the electromagnetic radiation source at step 1302. The illustrative process may stop at step 1314 after verifying the status of the container.

[0152] In practice, one or more steps shown in process 1300 may be combined with other steps,

performed in any suitable order, performed in parallel -- e.g., simultaneously or substantially simultaneously -- or deleted.

[0153] FIG. 14 shows user hand 1400 rendering tag 1402 inoperable by tearing tag 1402 along perforation 1408 to destroy coils 1404 of antenna 1406. Portion 1410 of tag 1402 may be detached from enclosure member 1420. Portion 1412 of tag 1402 may remain attached to enclosure member 1420. In some embodiments, by tearing tag 1402 along perforation 1408, the user interrupts electrical communication between the antenna and a storage device associated with tag 1402. This may effectively deactivate, or kill, the electrical circuit or tag.

[0154] FIG. 15 shows portion 1504 removed from enclosure member 1420 and portion 1502 remaining attached to enclosure member 1420. In some embodiments, all of tag 1402 (FIG. 14) may be removed from enclosure member 1420.

[0155] It will be noted that all of the features described above in connection with the decoupler of the invention may be applied to various types of containers and various types of assets in addition to the containers and assets described. The above described embodiments of the present invention are presented for the purposes of illustration and not of limitation, and the present invention is limited only by the claims which follow.

What is Claimed is:

1. A lockable container for securing an asset configured to be processed by an automatic container processing assembly having an optical sensor, the lockable container having a security status, the container comprising:

a first cover;

a second cover coupled to the first cover, wherein the first and second covers are configured to move between an open position which allows access to the asset, and a closed position which prevents access to the asset;

a locking member that is configured to move between an unlocked position, in which the first and second covers can move to the open position, and a locked position which locks the first and second covers in the closed position; and

a security status indicator that, when disposed in the assembly in a first position relative to the container, is configured to close an optical circuit between the indicator and the sensor and, when disposed in the assembly in a second position relative to the container, is configured to open the circuit.

2. The container of claim 1 wherein the security status indicator comprises a tag.

3. The container of claim 1 wherein the security status indicator exhibits a first reflectivity in the first position and a second reflectivity in the second position.

4. The container of claim 1 wherein the first position is indicative of the secure security status and the second position is indicative of the unsecure security status.

5. The container of claim 1 wherein the security status indicator comprises reflective foil.

6. The container of claim 1 wherein the security status indicator comprises reflective tape.

7. The container of claim 1 wherein the security status indicator comprises reflective ink.

8. The container of claim 1 wherein the sensor comprises a laser.

9. The container of claim 1 wherein the sensor comprises a light emitting diode.

10. A method for verifying the security status of a lockable container using a container processing assembly, the lockable container having a security status indicator configured to close an optical circuit between the indicator and an optical sensor in a first position and open the optical circuit in a second position, the method comprising:

aligning the security status indicator with an electromagnetic radiation source within the container processing assembly;

exposing the security status indicator to the electromagnetic radiation source;

detecting reflected electromagnetic radiation from the security status indicator; and

determining, from the detected reflected

electromagnetic radiation, whether the optical circuit is open or closed.

11. The method of claim 10 wherein detecting the reflected electromagnetic radiation comprises detecting the intensity of the reflected electromagnetic radiation.

12. The method of claim 10 wherein the electromagnetic radiation comprises visible light.

13. The method of claim 12 wherein detecting the reflected electromagnetic radiation comprises detecting the color of the visible light.

14. The method of claim 10 wherein aligning the security status indicator comprises moving the lockable container along a processing path.

15. The method of claim 14 wherein the processing path is mechanical.

16. The method of claim 10 wherein the security status indicator comprises reflective foil.

17. The method of claim 10 wherein the security status indicator comprises reflective tape.

18. The method of claim 10 wherein the security status indicator comprises reflective ink.

19. The method of claim 10 wherein exposing the security status indicator to the electromagnetic radiation source comprising shining a laser on the indicator.

20. The method of claim 10 wherein exposing the security status indicator to the electromagnetic radiation source comprises shining a light emitting diode on the indicator.

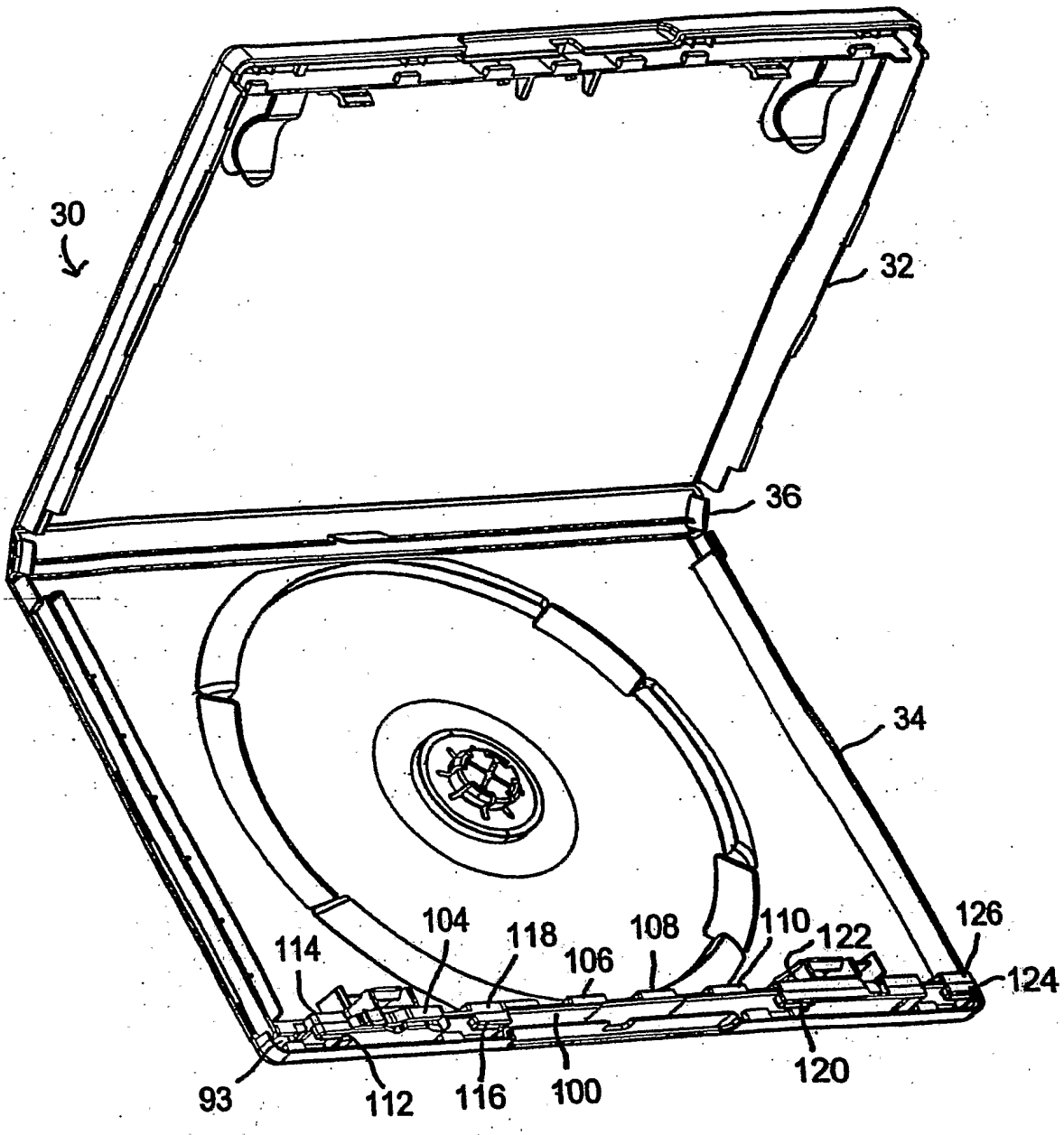


FIG. 1A

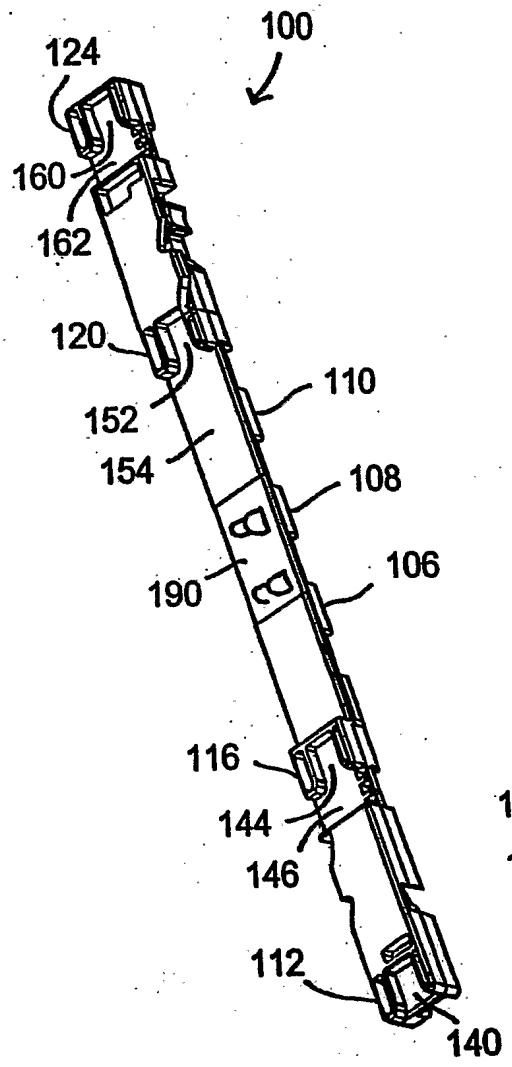

100
124
160
162
120
152
154
190
110
108
106
116
144
146
112
140

FIG. 1B

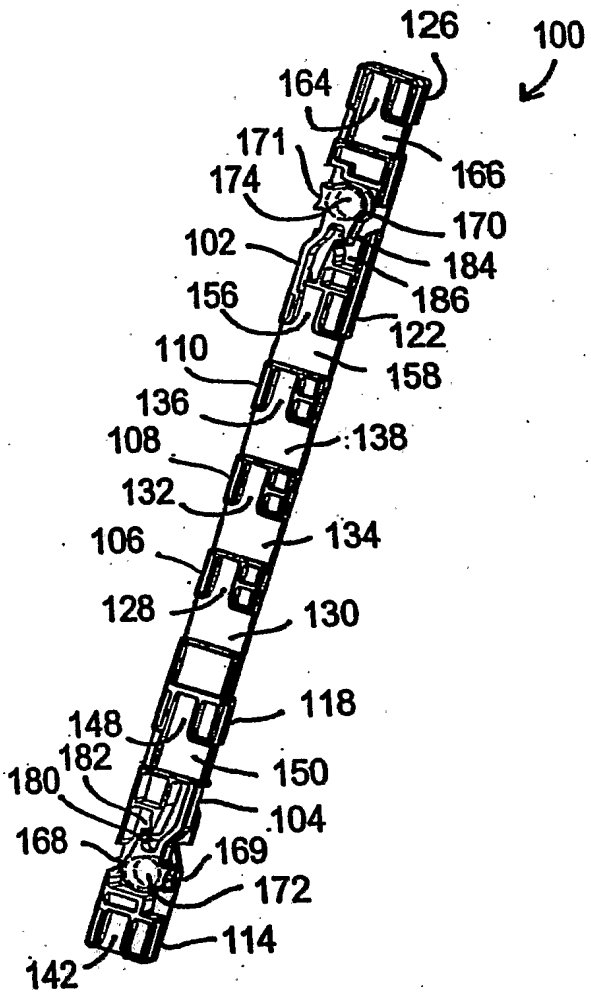

126
100
164
171
174
102
156
110
136
108
132
106
128
148
182
180
168
166
170
184
186
122
158
138
134
130
118
150
104
169
172
114
142

FIG. 1C

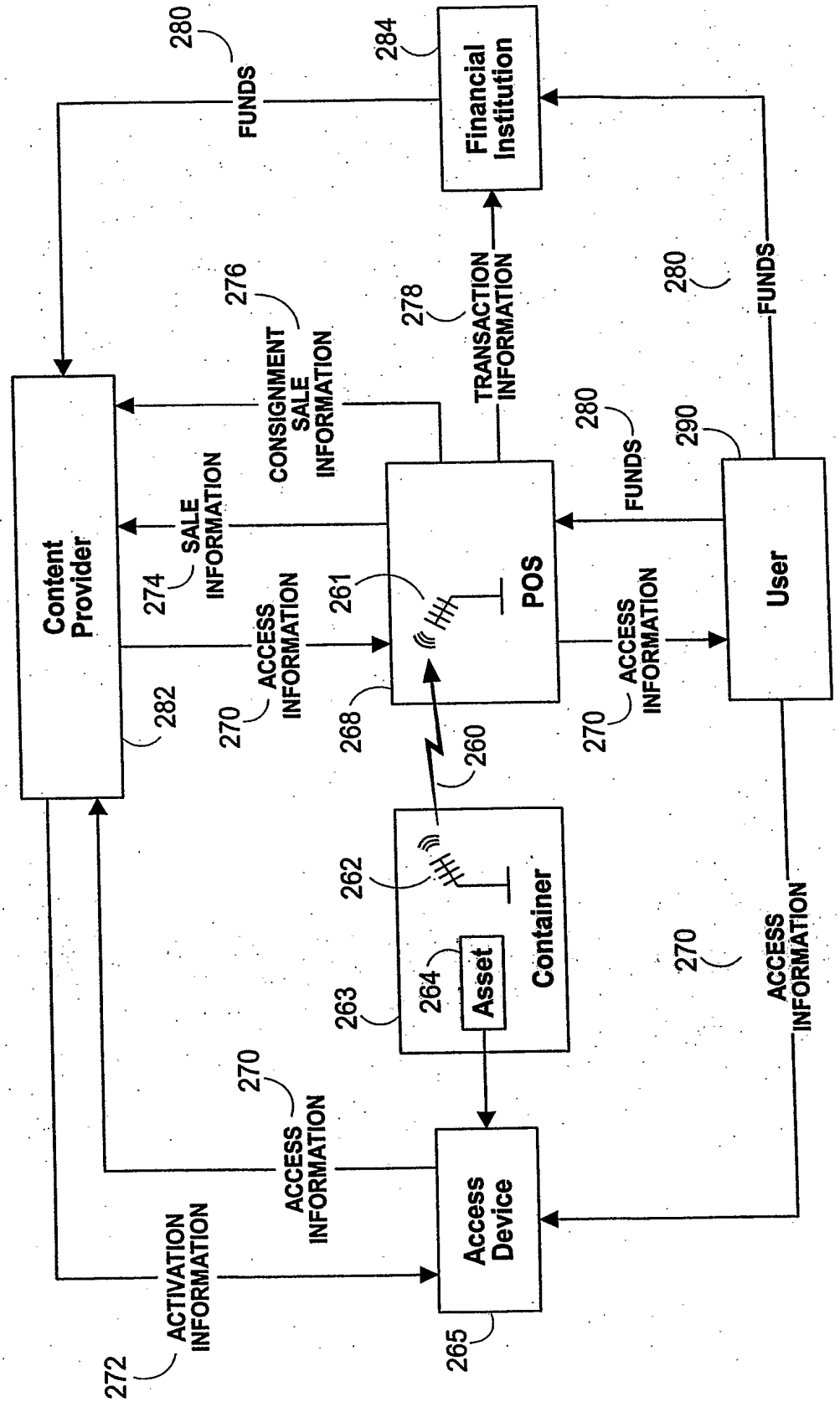

Financial Institution
284
FUNDS
280
Content Provider
282
CONSIGNMENT SALE INFORMATION
276
TRANSACTION INFORMATION
278
SALE INFORMATION
274
ACCESS INFORMATION
270
POS
261
268
260
User
290
FUNDS
280
ACCESS INFORMATION
270
Container
262
263
Asset
264
Access Device
265
ACCESS INFORMATION
270
ACTIVATION INFORMATION
272

FIG. 2A

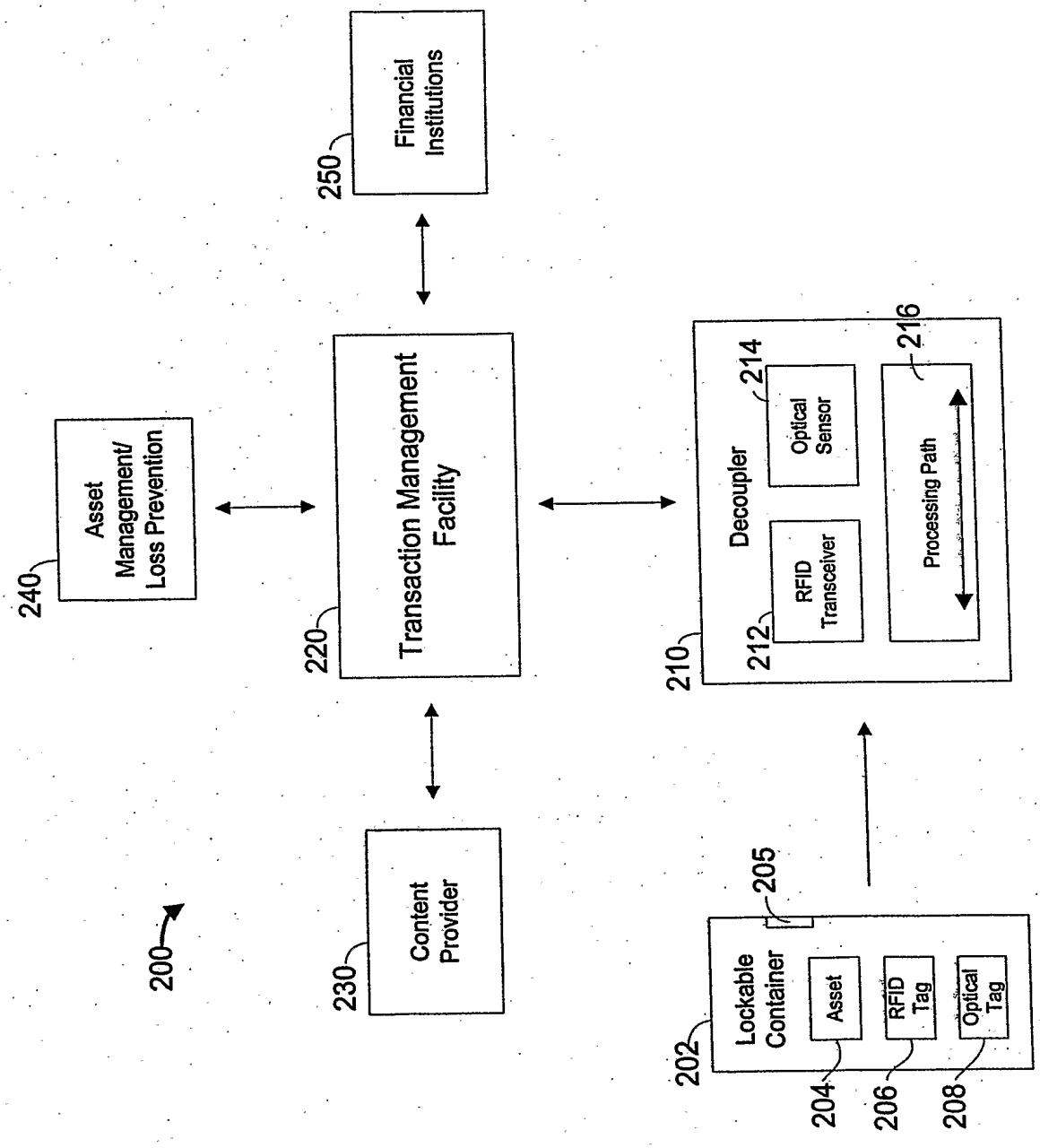

200
Financial Institutions
250
Asset Management/ Loss Prevention
240
Transaction Management Facility
220
Content Provider
230
Decoupler
210
Optical Sensor
214
RFID Transceiver
212
Processing Path
216
Lockable Container
202
205
Asset
204
RFID Tag
206
Optical Tag
208

FIG. 2B

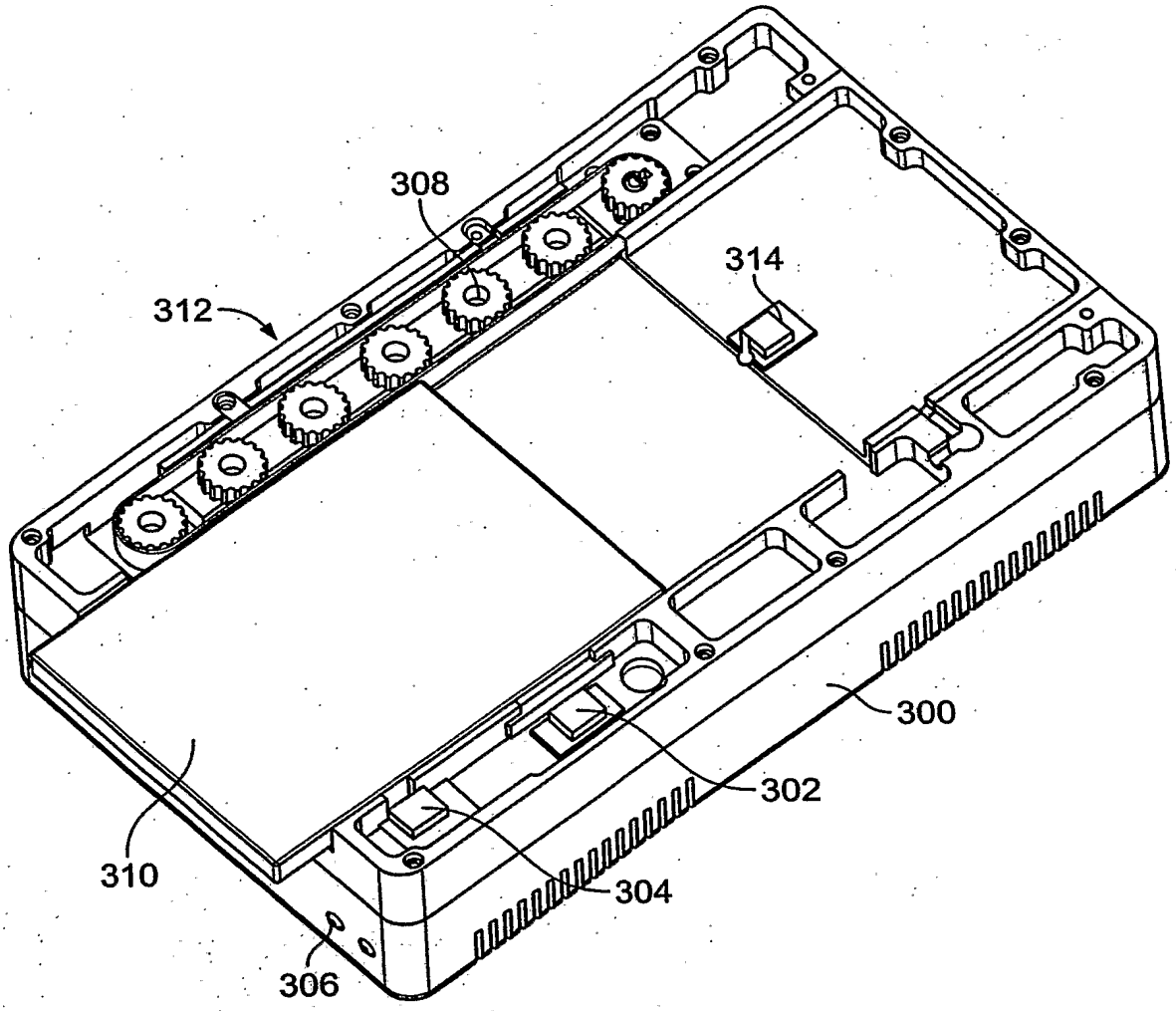


FIG. 3

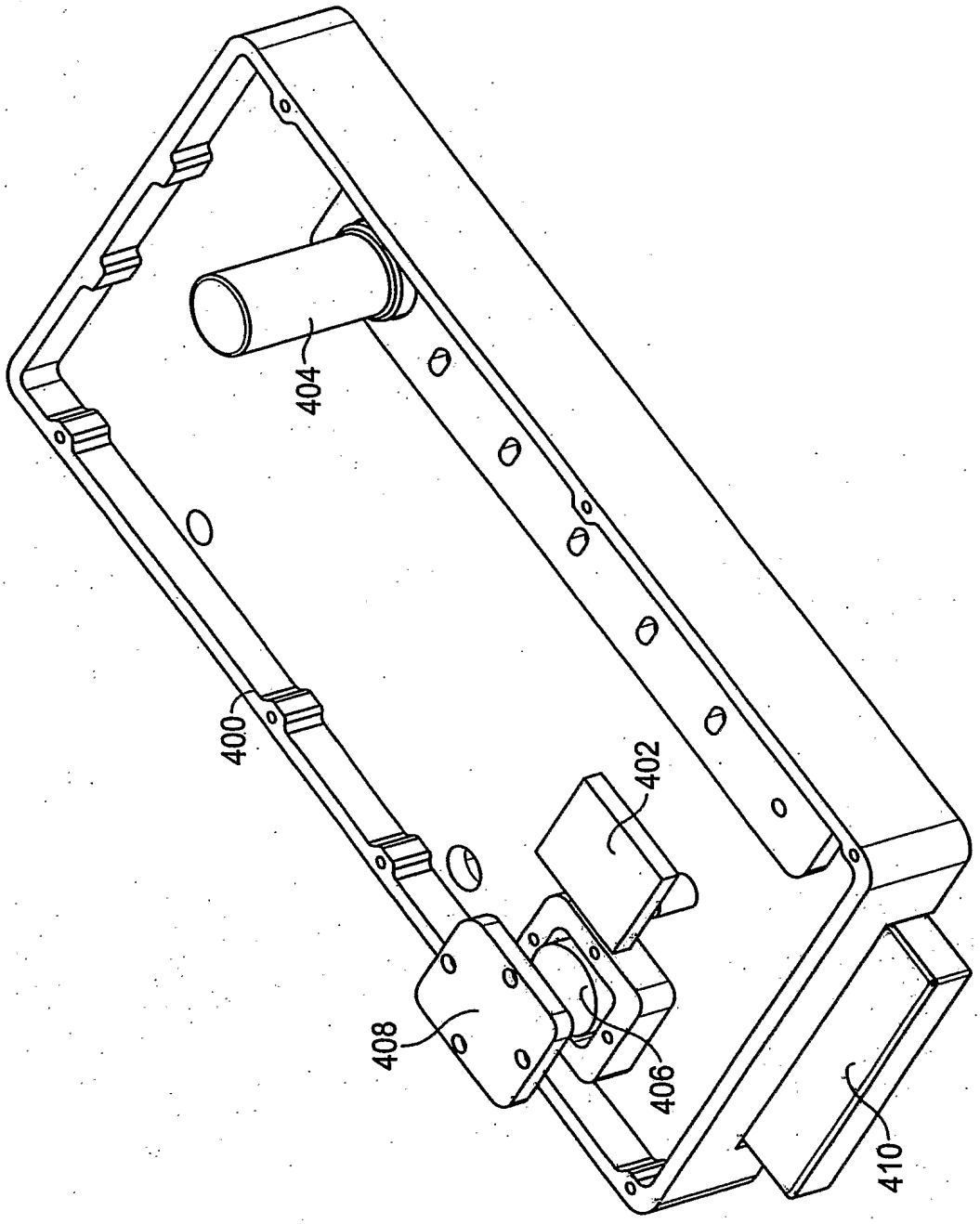


FIG. 4

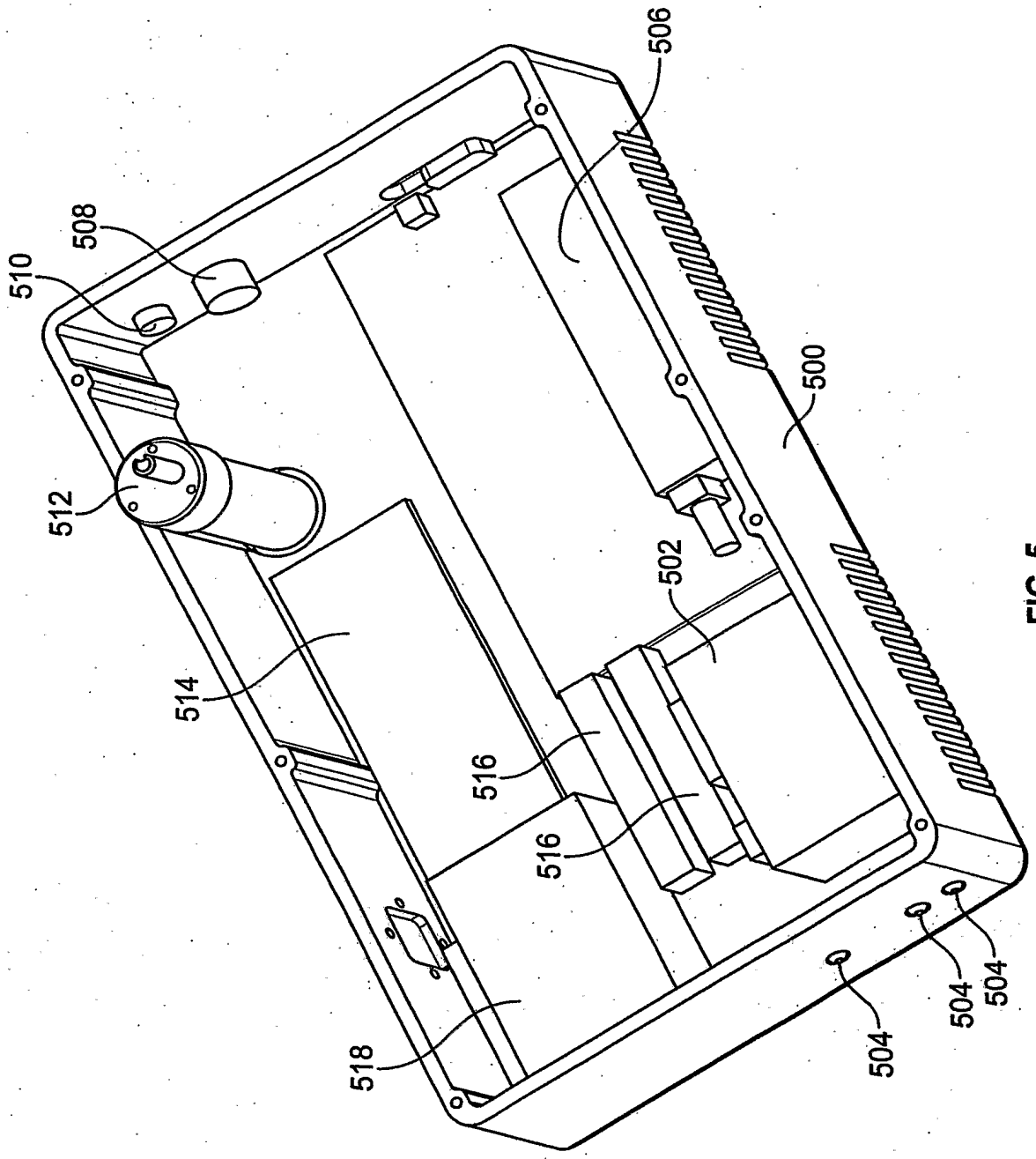


FIG. 5

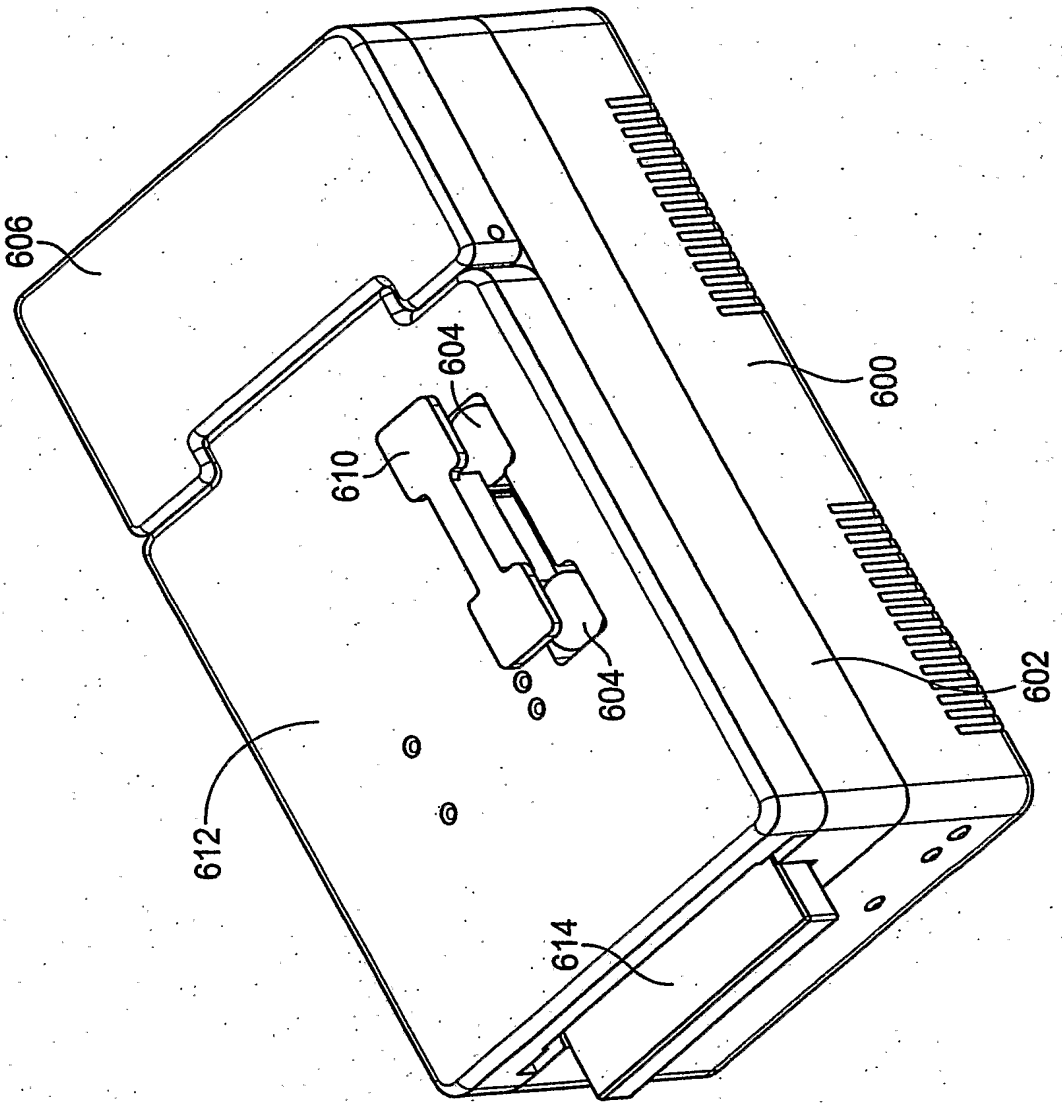


FIG. 6

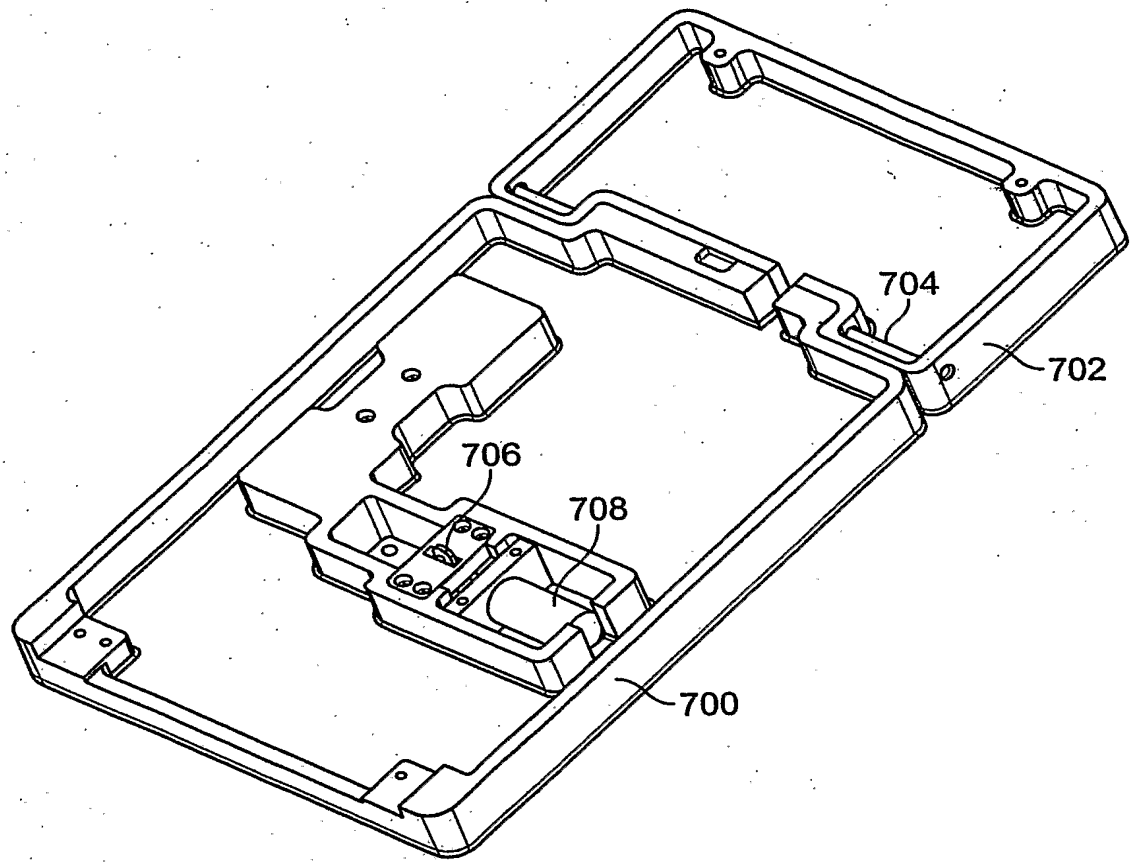


FIG. 7

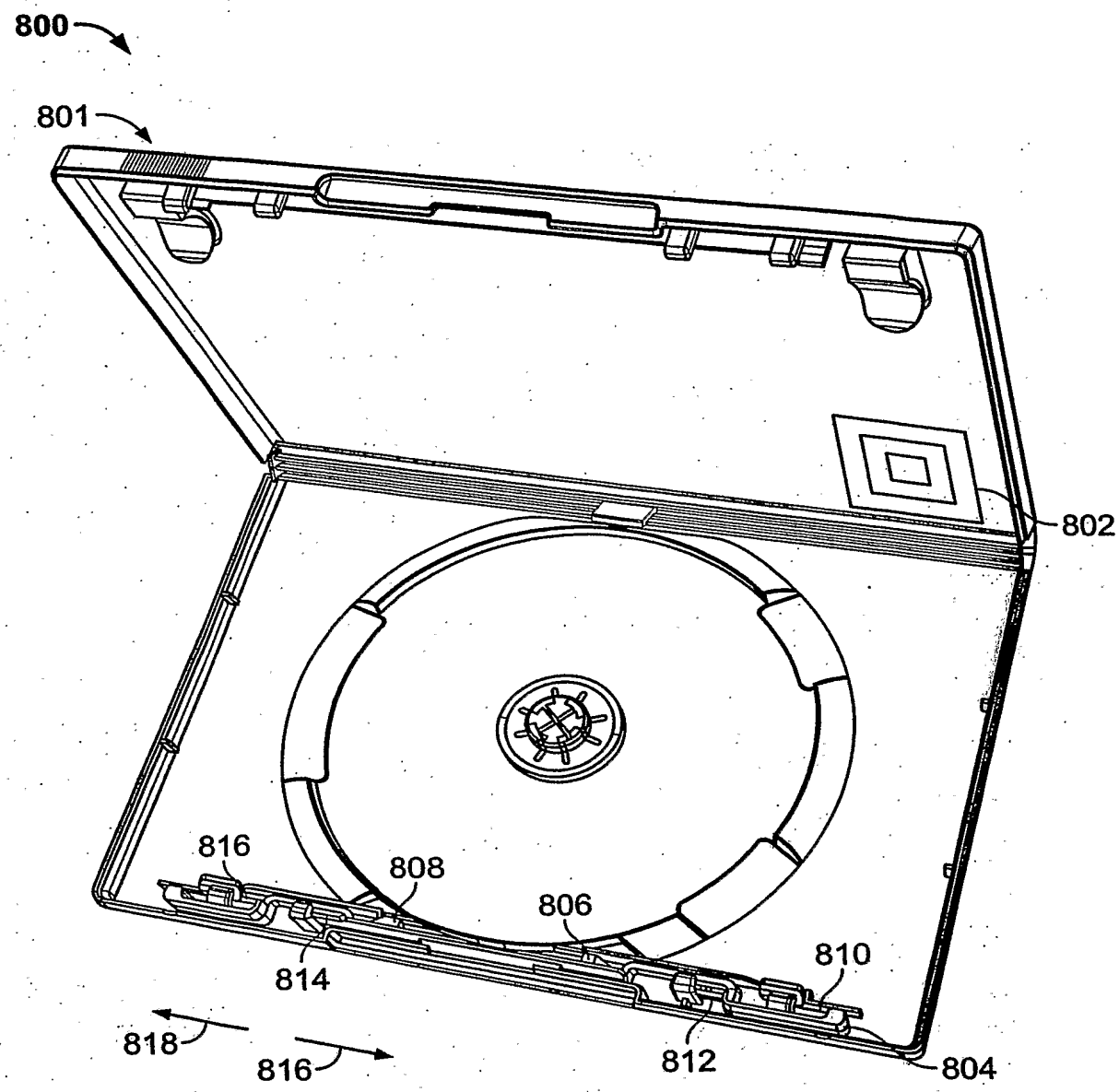


FIG. 8

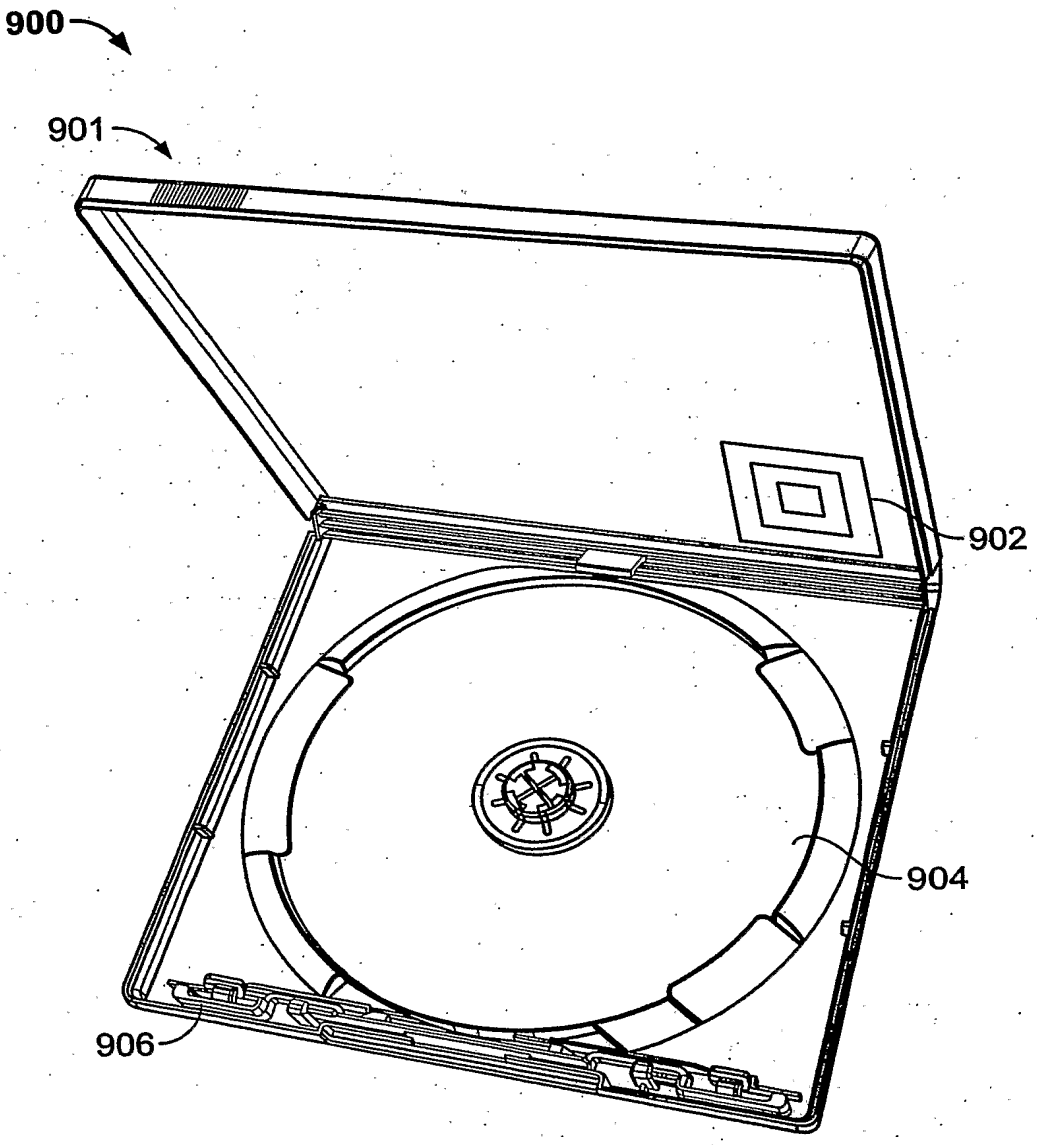


FIG. 9

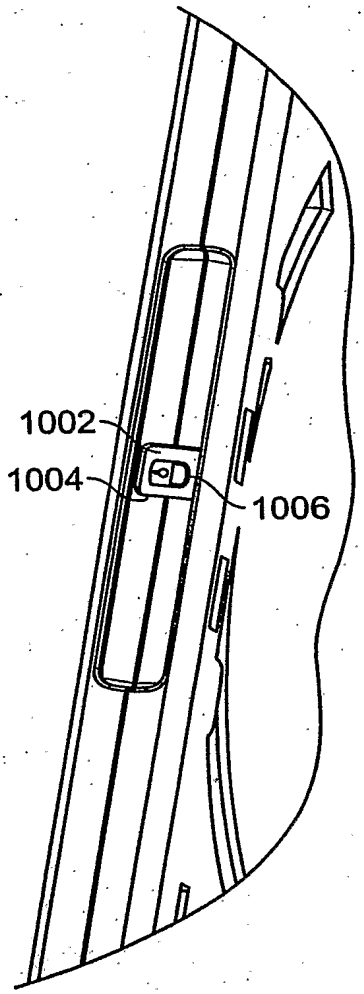


FIG. 10A

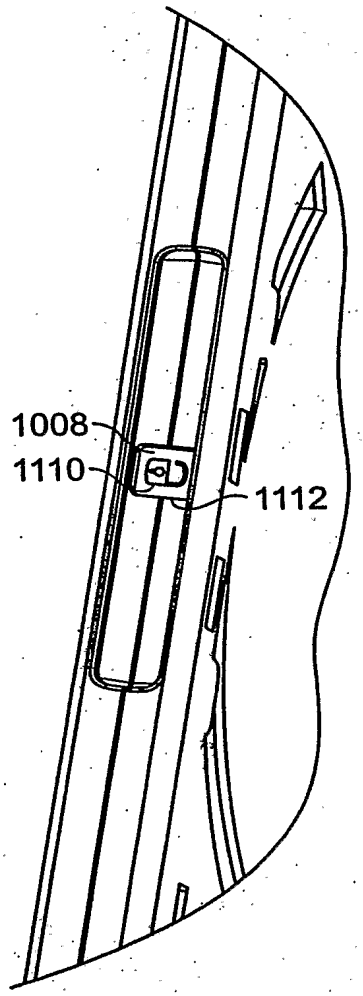


FIG. 10B

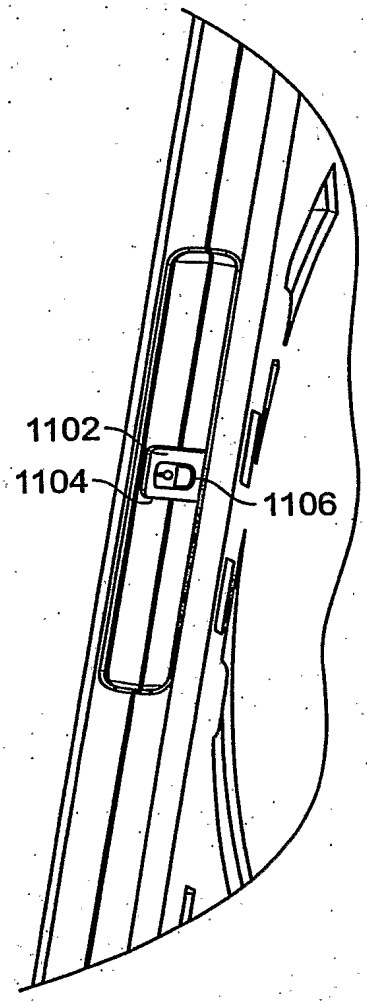


FIG. 11A

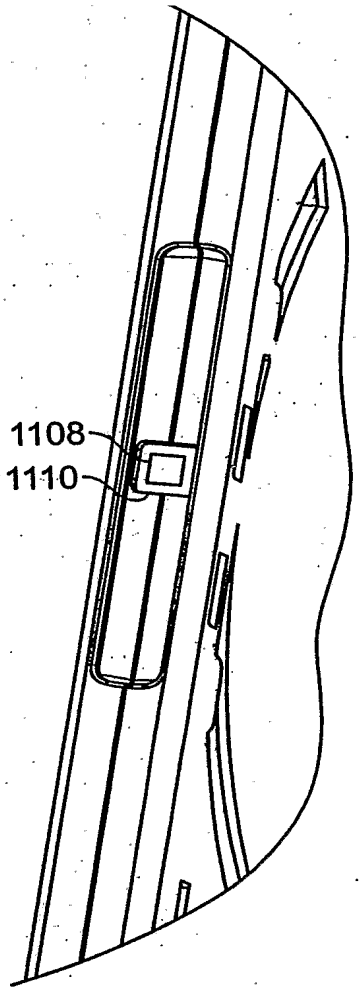


FIG. 11B

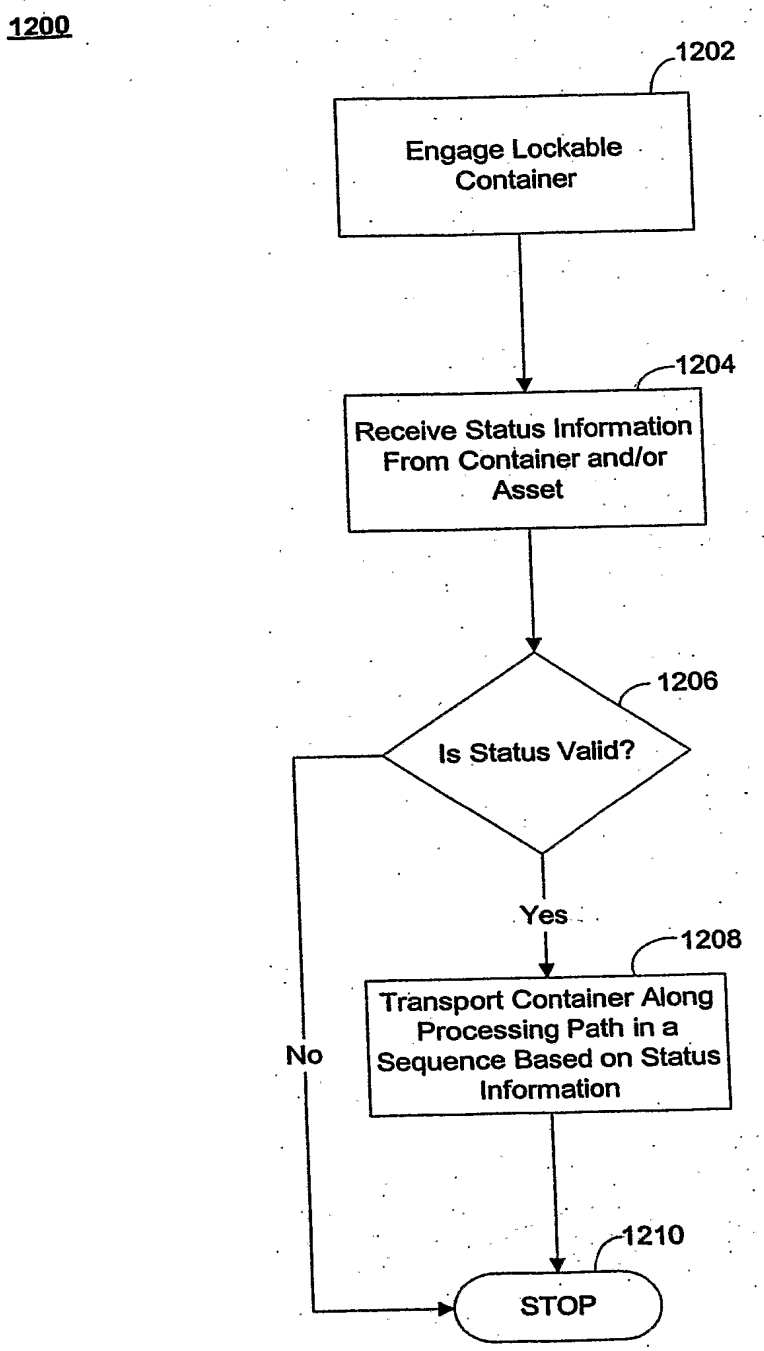

1200
1202
Engage Lockable Container
1204
Receive Status Information From Container and/or Asset
1206
Is Status Valid?
Yes
No
1208
Transport Container Along Processing Path in a Sequence Based on Status Information
1210
STOP

FIG. 12

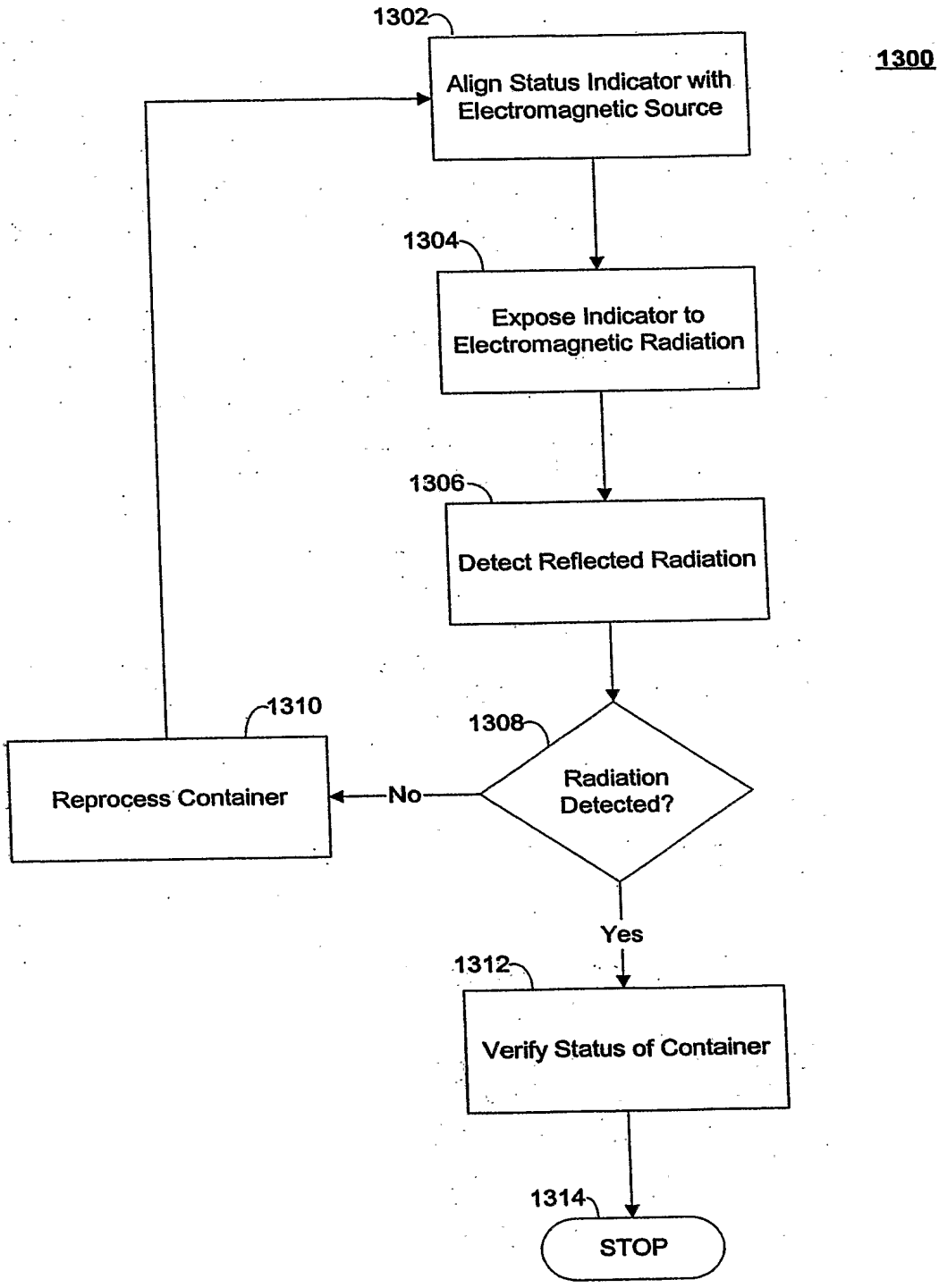

1300
1302
Align Status Indicator with Electromagnetic Source
1304
Expose Indicator to Electromagnetic Radiation
1306
Detect Reflected Radiation
1308
Radiation Detected?
No
1310
Reprocess Container
Yes
1312
Verify Status of Container
1314
STOP

FIG. 13

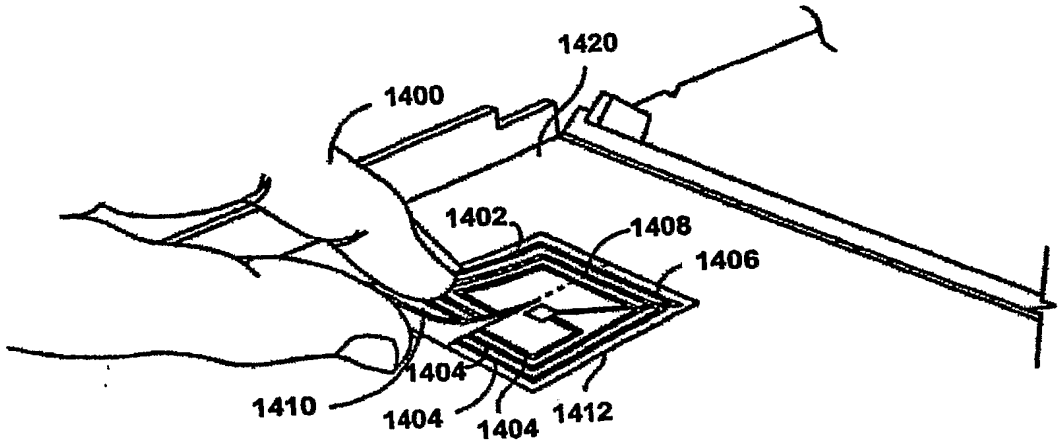

1420
1400
1402
1408
1406
1404
1410
1404
1404
1412

FIG. 14

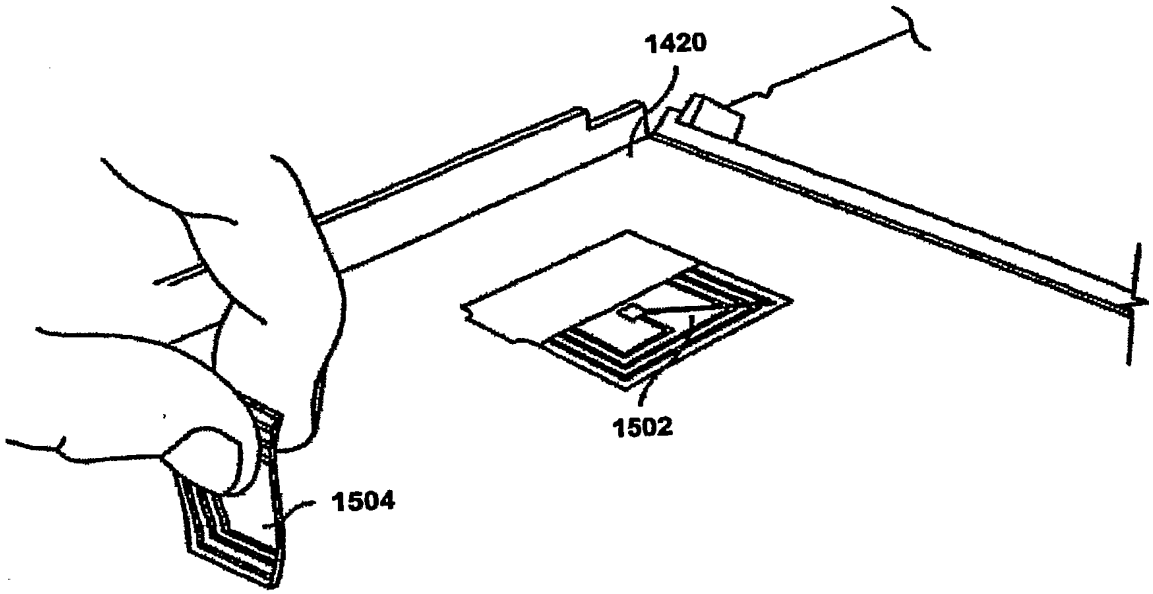

1420
1502
1504

FIG. 15

INTERNATIONAL SEARCH REPORT

In nal application No
PCT/US2005/042536

A. CLASSIFICATION OF SUBJECT MATTER
INV. E05B41/00 E05B73/00 G01V8/14 G11B33/04
ADD. E05B47/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
E05B G11B G01V G01N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 2004/129587 A1 (LAX MICHAEL R ET AL) 8 July 2004 (2004-07-08) cited in the application page 1, paragraph 3 - paragraph 10 page 4, paragraph 63 - paragraph 64 page 7, paragraph 92 - paragraph 93 page 8, paragraph 105 - page 9, paragraph 107 page 11, paragraph 133 - page 12, paragraph 138; figures	1-9 1,15
Y X	US 6 411 215 B1 (SHNIER J. MITCHELL) 25 June 2002 (2002-06-25) column 1, line 22 - column 13, line 39; figures	1-9 10-13, 17-20

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 March 2006	04/04/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Henkes, R

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 453 390 A (MORITZ ET AL) 12 June 1984 (1984-06-12)	1,3,4,7, 9
X	the whole document	10,12, 18,20

A	US 5 250 801 A (GROZINGER ET AL) 5 October 1993 (1993-10-05)	1,8,9, 11-13, 19,20
X	the whole document	10,14,15

A	US 4 772 877 A (RICE, JR. ET AL) 20 September 1988 (1988-09-20) column 7, line 1 - line 17	1,5,9, 10,16,20

A	US 2003/193883 A1 (PARKS WILLIAM S ET AL) 16 October 2003 (2003-10-16)	1
X	the whole document	10-14,19

INTERNATIONAL SEARCH REPORT

nformation on patent family members

International application No
PCT/US2005/042536

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004129587 A1	08-07-2004	AU 2004200405 A1	26-08-2004
		CA 2456995 A1	07-08-2004
		CN 1539717 A	27-10-2004
		EP 1445406 A2	11-08-2004
US 6411215 B1	25-06-2002	NONE	
US 4453390 A	12-06-1984	AU 7921082 A	22-07-1982
		CA 1172724 A1	14-08-1984
		GB 2093520 A	02-09-1982
		JP 57140480 A	31-08-1982
US 5250801 A	05-10-1993	DE 4031142 A1	09-04-1992
		DK 503040 T3	22-05-1995
		WO 9206387 A1	16-04-1992
		EP 0503040 A1	16-09-1992
		JP 5502729 T	13-05-1993
US 4772877 A	20-09-1988	NONE	
US 2003193883 A1	16-10-2003	US 2003193885 A1	16-10-2003